

# New Features Guide

## FortiAnalyzer 7.0.0



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



July 15, 2021

FortiAnalyzer 7.0.0 New Features Guide

05-700-698019-20210715

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>FortiAnalyzer 7.0.0 New Features Guide</b>	<b>6</b>
<b>Device Manager</b>	<b>7</b>
Device and Groups	7
World map added to the Device Manager	7
Model device support for central logging	9
SD-WAN	11
Improved secure SD-WAN monitor	11
<b>Security Operations (SOC)</b>	<b>15</b>
SOC automation	15
FortiOS connector health check	15
Attach FortiMail connector actions to incidents	18
SIEM correlation and analysis	23
Importing and exporting playbooks	25
FortiGuard outbreak and alert service	26
Manage subnets	30
Incident and Event Management	31
FortiClient event handler update	32
FortiDeceptor default handler	33
IPS signatures on-hold event handler	34
NOC event handlers	36
Dashboards	39
Shadow IT Monitoring Service	39
Data sources tuning	42
Asset and Identity Dashboards	46
<b>Log and Report</b>	<b>50</b>
Logging	50
Improve log forwarding bandwidth efficiency	50
Per-device log receiving rate limit	53
Mask user data in log forwarder	55
FortiEDR Central Manager logging	58
FortiAI logging on FortiAnalyzer 7.0.1	60
Log forwarding enhancement 7.0.1	64
Reports	65
Improved caching mechanism for reports	65
FortiDeceptor report	68
Central UEBA table for custom reporting and widgets	69
FortiSandbox CTAP report	70
Organize reports in folders	72
Additional charts for SD-WAN reporting 7.0.1	75
<b>System</b>	<b>81</b>
High Availability (HA)	81
FortiAnalyzer HA graceful upgrade	81
Administrators	83

---

Theme mode .....	84
Add operation permissions to Admin profile .....	85
Admins can use a SAML SSO FortiCloud account to log in to FortiAnalyzer .....	89
ADOM .....	91
Support for link aggregation .....	92
<b>Management Extensions .....</b>	<b>96</b>
New management extension - FortiSOAR .....	96
<b>Other .....</b>	<b>100</b>
FortiAnalyzer Setup wizard .....	100
FortiAnalyzer VM licenses .....	104
Requesting and activating a trial license .....	104
Activating a new license .....	107
Activating an add-on license .....	108
FortiAnalyzer Federation .....	110
Device Manager .....	110
FortiSoC .....	111
Configure FortiAnalyzer Federation in the CLI .....	116
Limitations .....	116
CSF support for multiple VDOMs .....	117
Event log easier to read 7.0.1 .....	117



# Change Log

Date	Change Description
2021-04-22	Initial release of FortiAnalyzer 7.0.0.
2021-04-23	Added <a href="#">Data sources tuning on page 42.</a>
2021-04-29	Updated <a href="#">Shadow IT Monitoring Service on page 39.</a>
2021-04-30	Added: <ul style="list-style-type: none"><li>• <a href="#">FortiAnalyzer Federation on page 110</a></li><li>• <a href="#">Admins can use a SAML SSO FortiCloud account to log in to FortiAnalyzer on page 89</a></li></ul>
2021-05-10	Added <a href="#">CSF support for multiple VDOMs on page 117.</a>
2021-05-26	Added <a href="#">Improved secure SD-WAN monitor on page 11.</a>
2021-07-15	Added <a href="#">FortiAnalyzer HA graceful upgrade on page 81.</a>
2021-07-15	Initial release of FortiAnalyzer 7.0.1.

# FortiAnalyzer 7.0.0 New Features Guide

This document describes the new features added to FortiAnalyzer 7.0.0. The FortiAnalyzer new features are organized into the following categories:

- [Device Manager on page 7](#)
- [Security Operations \(SOC\) on page 15](#)
- [Log and Report on page 50](#)
- [System on page 81](#)
- [Management Extensions on page 96](#)
- [Other on page 100](#)

# Device Manager

This section lists the new features added to FortiAnalyzer for the device manager:

- [Device and Groups on page 7](#)
- [SD-WAN on page 11](#)

## Device and Groups

This section lists the new features added to FortiAnalyzer for devices and groups:

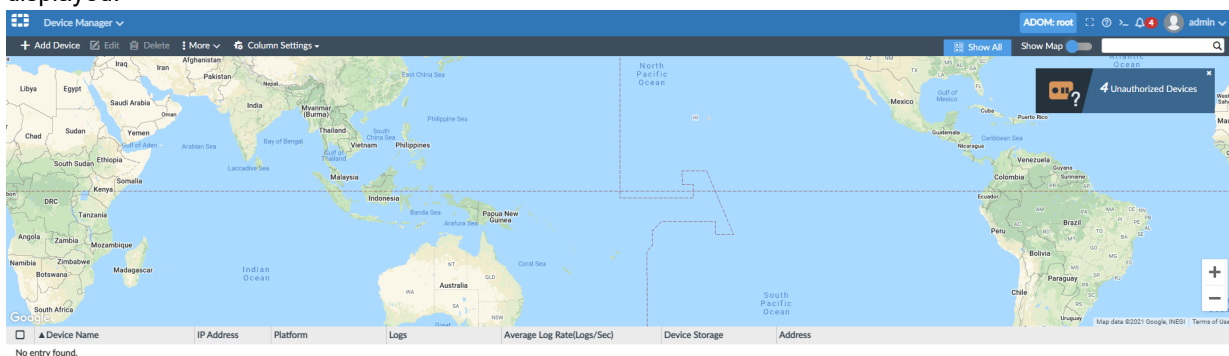
- [World map added to the Device Manager on page 7](#)
- [Model device support for central logging on page 9](#)

## World map added to the Device Manager

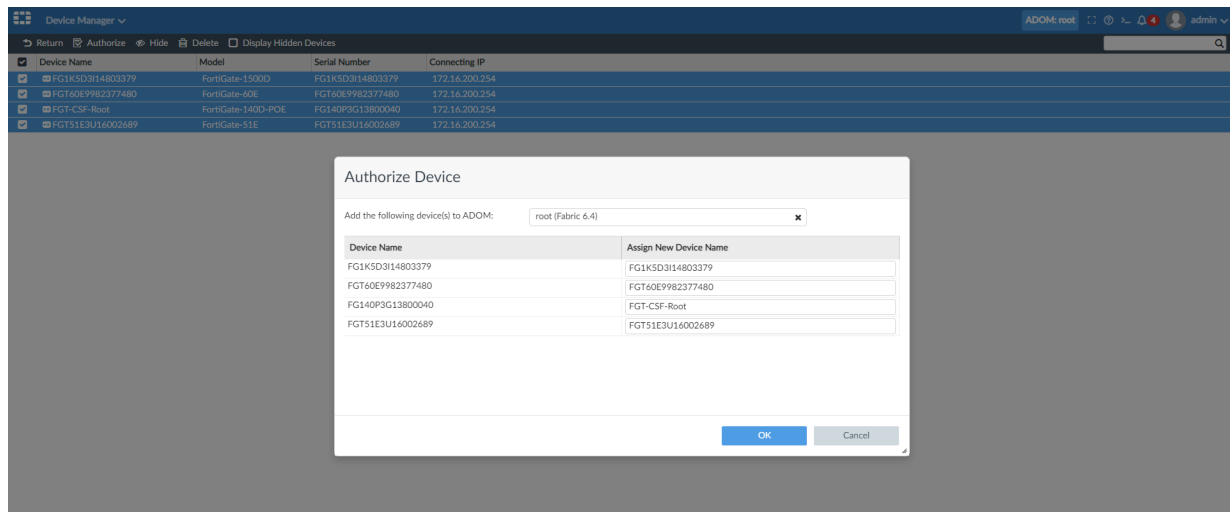
An enhancement to the Device Manager page which shows the locations of the registered device in a world map.

**To view the world map in Device Manager:**

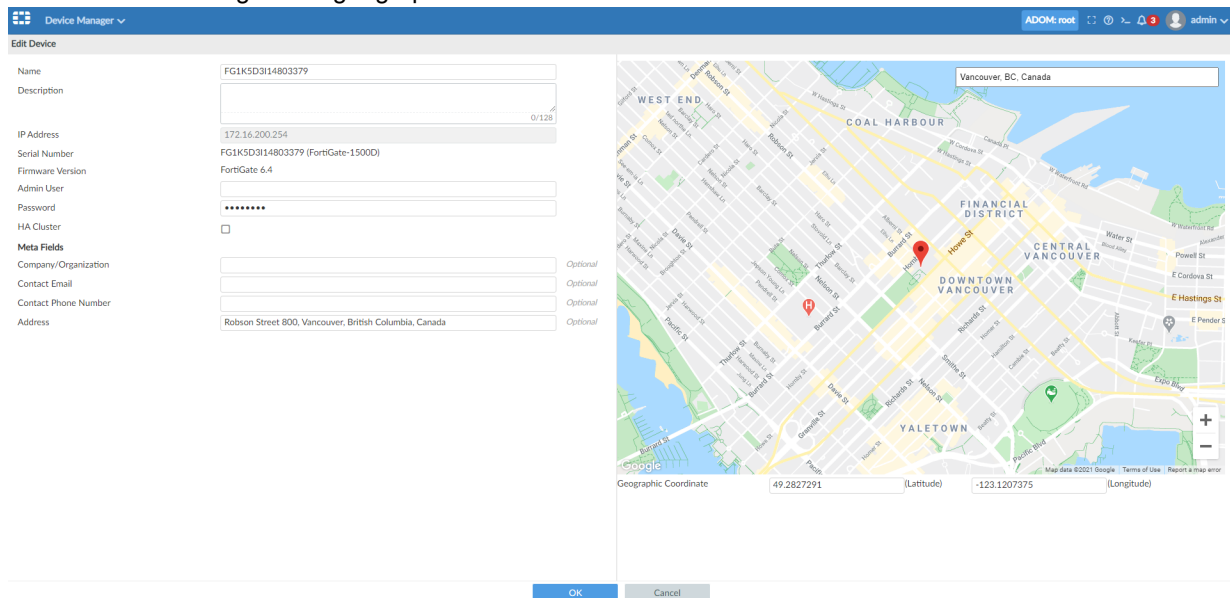
1. Go to Device Manager in the FortiAnalyzer GUI. By default, the *Show Map* toggle is enabled and the map is displayed.



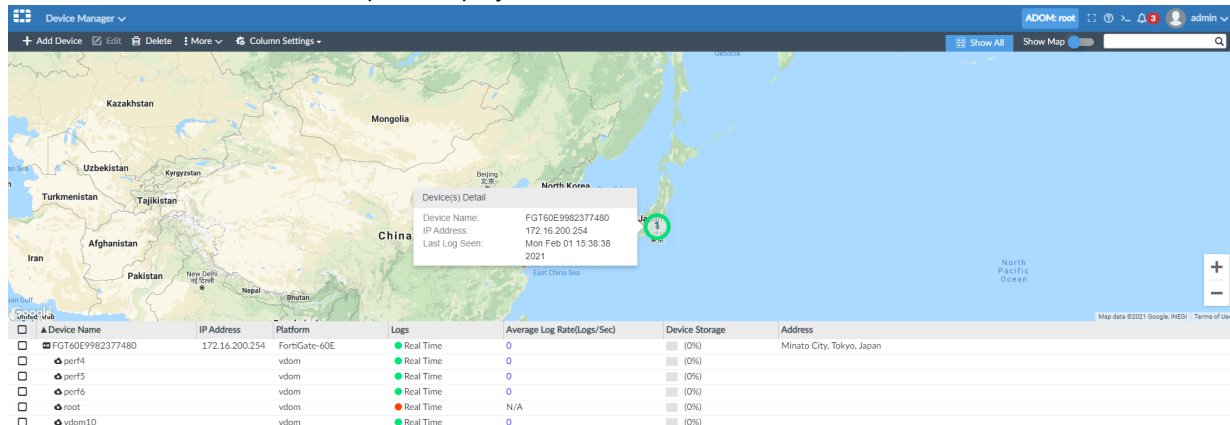
When there are unregistered devices, a small *Unauthorized Devices* window is displayed on the map. Click *Unauthorized Devices* to view all unauthorized devices in a table. Administrators are able to authorize devices from this view. Click *Return* to view authorized devices and the map.



## 2. Edit a device to configure the geographic coordinates for each device.



Configured device locations are displayed on the world map. You can zoom in or out on the world map. Only the devices that are visible in the map are displayed in the table below.



3. To disable the world map, set the Show Map toggle to the off position. When the world map is disabled, the device table displays all authorized devices.

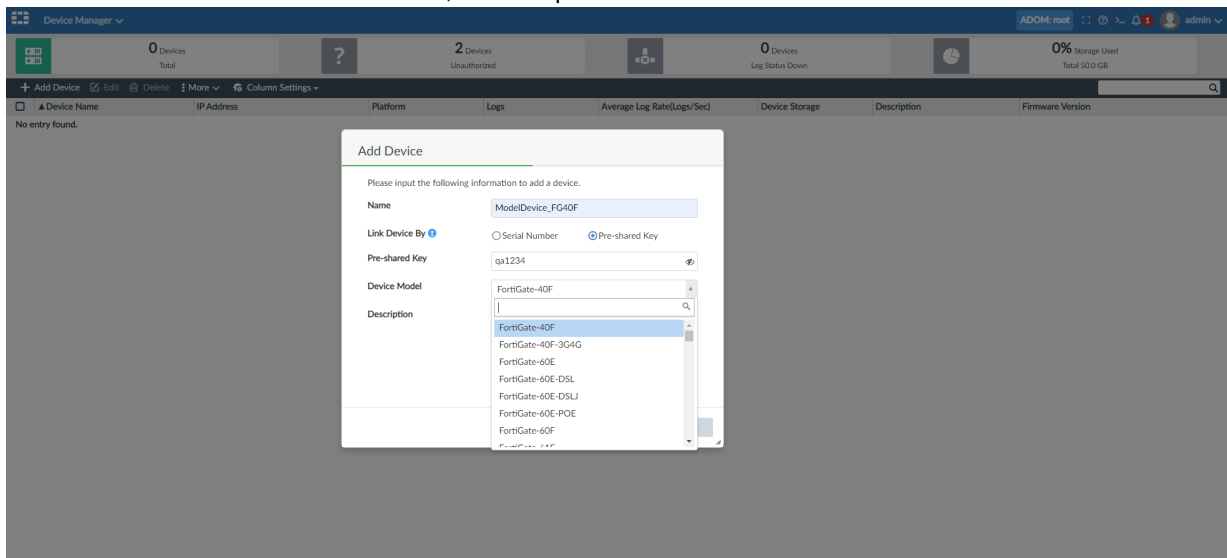
Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Address
FG1K5D314803379	172.16.200.254	FortiGate-1500D	Real Time	0	(0%)	Robson Street 800, Vancouver, British Columbia, Canada
FGT60E982377480	172.16.200.254	FortiGate-60E	Real Time	0	(0%)	Minato City, Tokyo, Japan
per4		vdom	Real Time	0	(0%)	
per5		vdom	Real Time	0	(0%)	
per6		vdom	Real Time	0	(0%)	
root		vdom	Real Time	N/A	(0%)	
vdom10		vdom	Real Time	0	(0%)	
FGT-CSF-Root*	172.16.200.254	FortiGate-140D-POE	Real Time	0	(39.04%)	José María Pino Suárez 29, Ciudad de México, Ciudad de México, Mexico
FGT51E3U16002689	172.16.200.254	FortiGate-51E	Real Time	0	(4.3%)	Broadway 240, New York, New York, United States

## Model device support for central logging

FortiAnalyzer includes the option to add a device as a model device in *Device Manager* and auto-link the device using a pre-shared key when the real device connects to FortiAnalyzer.

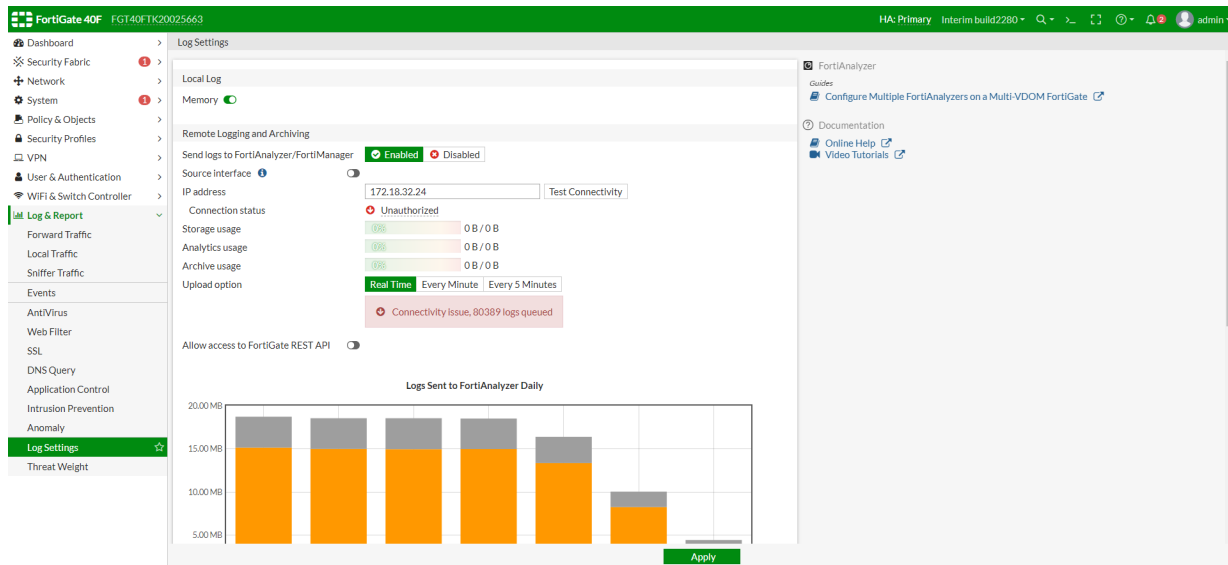
### To add devices using a pre-shared key:

1. On FortiAnalyzer, go to the *Device Manager*, and click *Add Device*.
2. Under *Link Device By* select *Pre-shared Key*, configure the settings for your device, and click *Next*.
  - a. **Name:** Enter a name for the device, for example, *ModelDevice\_FG40F*.
  - b. **Pre-shared Key:** Enter a pre-shared key, for example: *qa1234*.
  - c. **Device Model:** Select the device model, for example: *FGT40F*.

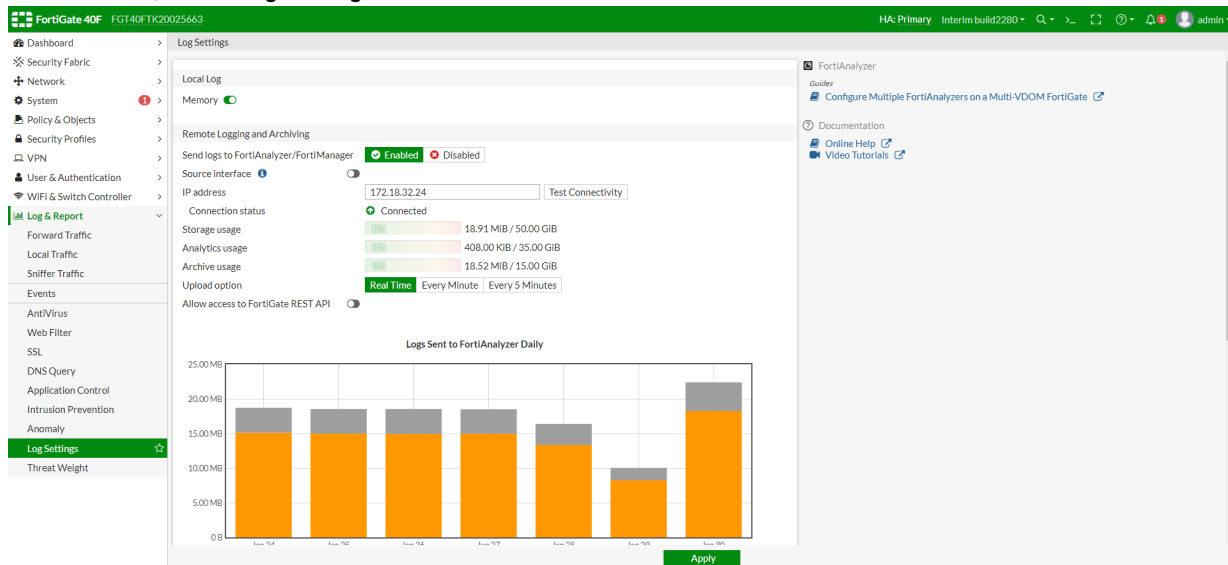


The device is added successfully but is not yet authorized.

3. On the FortiGate, go to *Log Settings* to configure the FortiAnalyzer. At this time, the connection status is unauthorized.



4. In the FortiGate CLI, configure the pre-shared key to match the one configured on the FortiAnalyzer, for example qa1234.
- ```
config log fortianalyzer setting
set preshared-key <your pre-shared key>
```
5. On FortiAnalyzer, go to the *Device Manager* and refresh the table. The FortiGate device is recognized and is automatically authorized as a registered device.
6. On FortiGate, check *Log Settings* to confirm the connection status is *Connected*.



### To add multiple devices using the same FortiGate platform:

1. On FortiAnalyzer, go to the *Device Manager* and configure multiple model devices using the same FortiGate platform. Each configured device must have a unique pre-shared key. In this example, five devices are configured.

| + Add Device Edit Delete More Column Settings |             |               |                  |                            |                |             |                           |  |
|-----------------------------------------------|-------------|---------------|------------------|----------------------------|----------------|-------------|---------------------------|--|
| Device Name                                   | IP Address  | Platform      | Logs             | Average Log Rate(Logs/Sec) | Device Storage | Description | Firmware Version          |  |
| ModelDevice_FG40F                             | 172.16.81.1 | FortiGate-40F | Real Time        | N/A                        | (0.04%)        |             | FortiGate 6.6.0 (Interim) |  |
| ModelDevice_FG60E1                            |             | FortiGate-60E | Store And Upload | N/A                        | (0%)           |             | FortiGate 6.4             |  |
| ModelDevice_FG60E2                            |             | FortiGate-60E | Store And Upload | N/A                        | (0%)           |             | FortiGate 6.4             |  |
| ModelDevice_FG60E3                            |             | FortiGate-60E | Store And Upload | N/A                        | (0%)           |             | FortiGate 6.4             |  |
| ModelDevice_FG60E4                            |             | FortiGate-60E | Store And Upload | N/A                        | (0%)           |             | FortiGate 6.4             |  |
| ModelDevice_FG60E5                            |             | FortiGate-60E | Store And Upload | N/A                        | (0%)           |             | FortiGate 6.4             |  |

- When a corresponding FortiGate device is configured to send logs to the FortiAnalyzer, and it is configured with a pre-shared key matching one of the five configured in FortiAnalyzer, it is automatically authorized as a registered device on FortiAnalyzer.

| + Add Device Edit Delete More Column Settings |             |               |                  |                            |                |             |                           |  |
|-----------------------------------------------|-------------|---------------|------------------|----------------------------|----------------|-------------|---------------------------|--|
| Device Name                                   | IP Address  | Platform      | Logs             | Average Log Rate(Logs/Sec) | Device Storage | Description | Firmware Version          |  |
| ModelDevice_FG40F                             | 172.16.81.1 | FortiGate-40F | Real Time        | N/A                        | (0.04%)        |             | FortiGate 6.6.0 (Interim) |  |
| ModelDevice_FG60E1                            |             | FortiGate-60E | Store And Upload | N/A                        | (0%)           |             | FortiGate 6.4             |  |
| ModelDevice_FG60E2                            |             | FortiGate-60E | Store And Upload | N/A                        | (0%)           |             | FortiGate 6.4             |  |
| ModelDevice_FG60E3                            | 172.16.81.1 | FortiGate-60E | Real Time        | N/A                        | (0.01%)        |             | FortiGate 6.4             |  |
| ModelDevice_FG60E4                            |             | FortiGate-60E | Store And Upload | N/A                        | (0%)           |             | FortiGate 6.4             |  |
| ModelDevice_FG60E5                            |             | FortiGate-60E | Store And Upload | N/A                        | (0%)           |             | FortiGate 6.4             |  |

## SD-WAN

This section lists the new features added to FortiAnalyzer for SD-WAN:

- Improved secure SD-WAN monitor on page 11

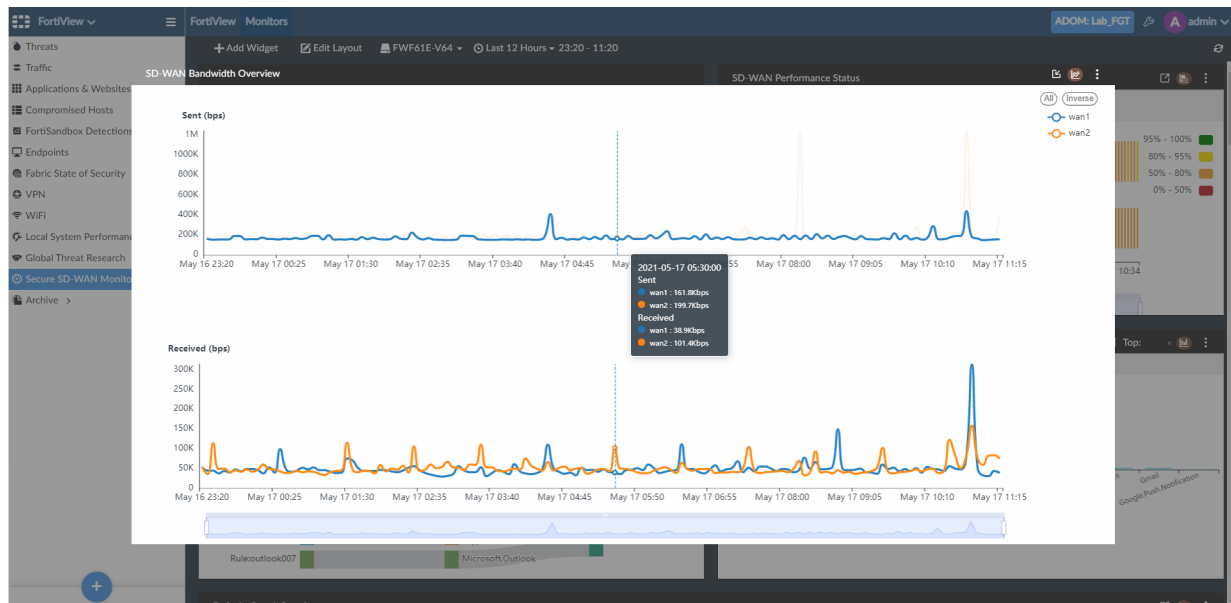
### Improved secure SD-WAN monitor

This is an enhancement to the existing Secure SD-WAN Monitor dashboard by providing more widgets and detailed information.

**To view the secure SD-WAN monitor enhancements:**

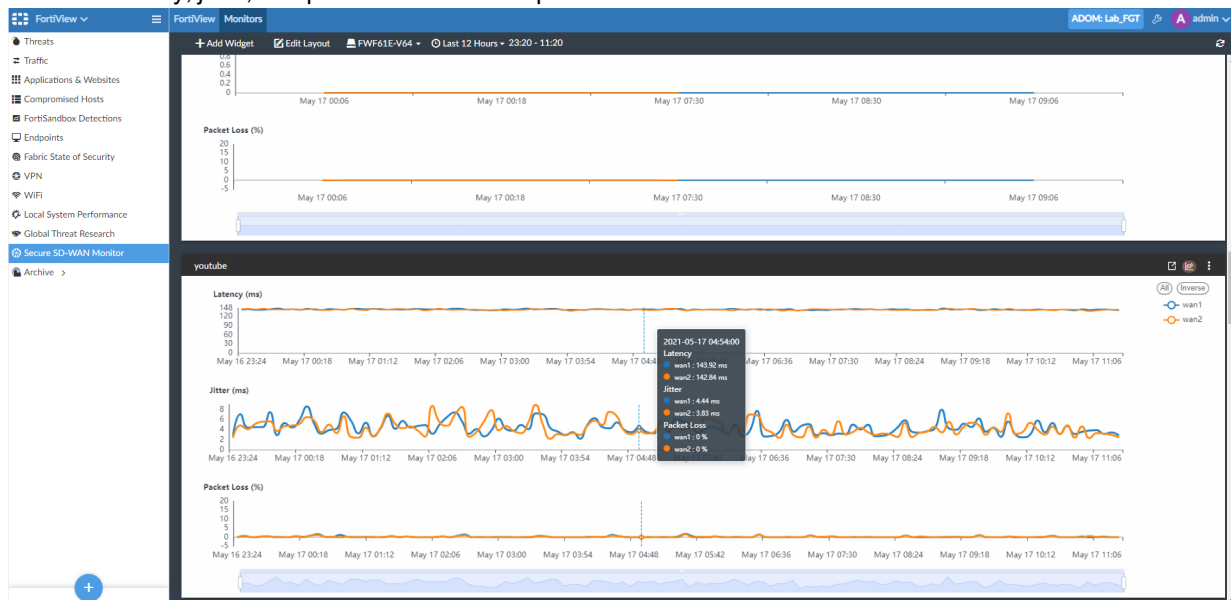
- Go to *FortiView > Monitors > Secure SD-WAN Monitor*.

A new widget called *SD-WAN Bandwidth Overview* has been added which displays a line chart of the sent/received rate (bps) in the selected time period for SD-WAN members interfaces. In this widget, users can select or deselect member interfaces and mouse over the line chart to view the sent/received rate in a tooltip for the selected interfaces.



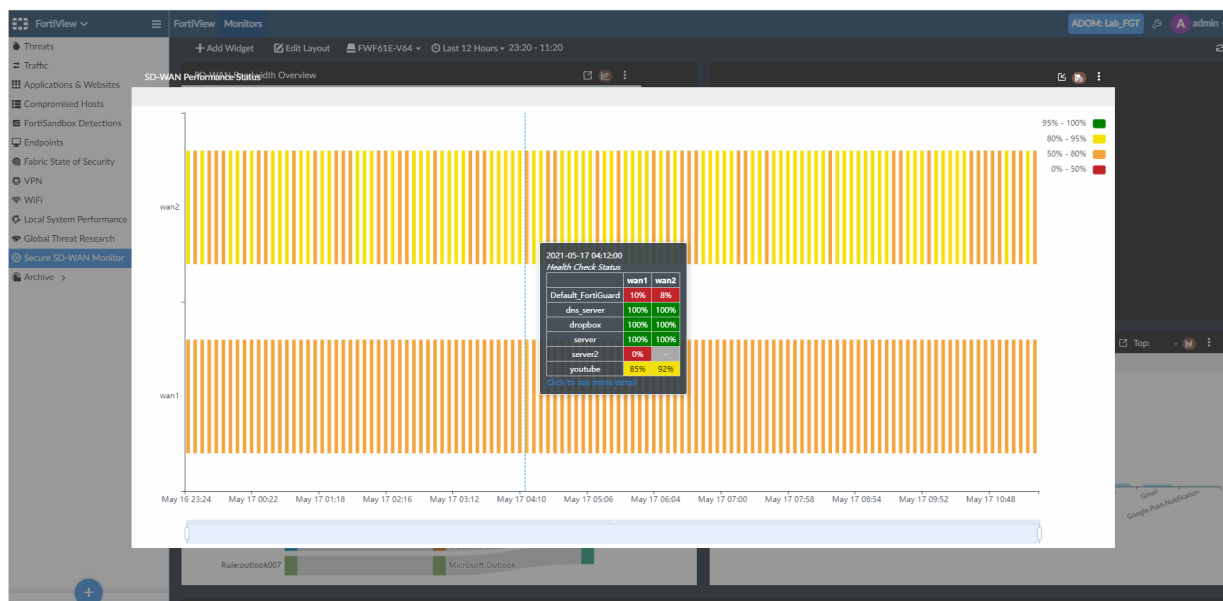
The *Latency*, *Jitter*, and *Packet Loss* widgets have been replaced with the new *Health Check Status* widget. This widget dynamically creates a child-widget for each health check where a line chart of latency, jitter, and packet loss in the selected time period for SD-WAN interfaces is displayed.

In each *Health Check Status* widget, users can select/deselect member interfaces and mouse over line charts to view the latency, jitter, and packet loss in a tooltip for the selected interface.

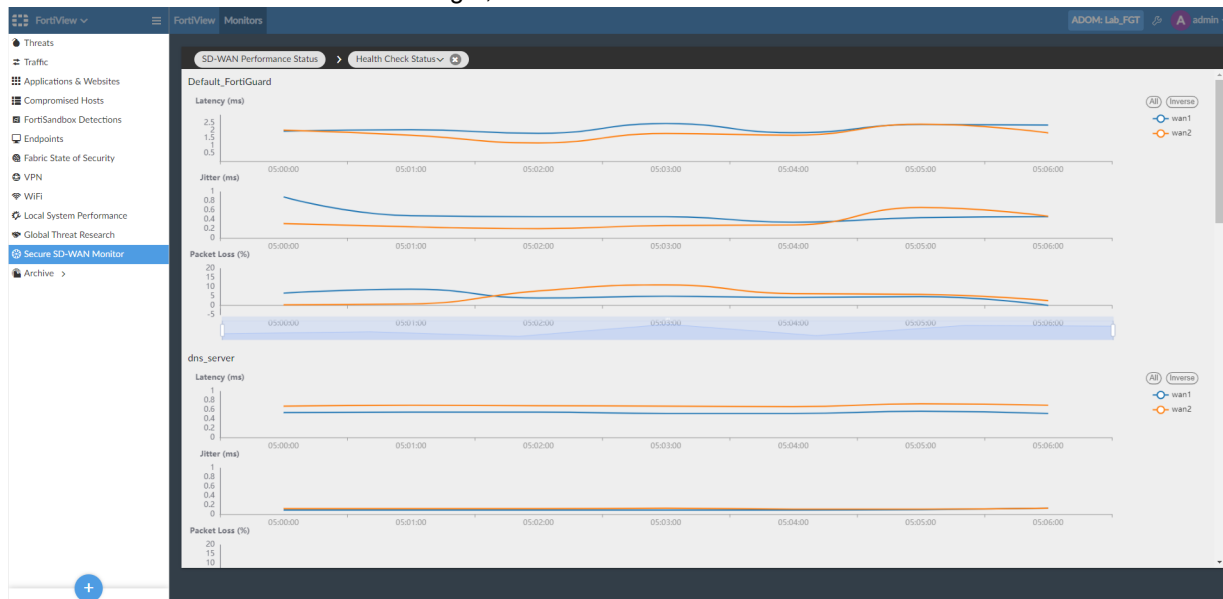


In the *SD-WAN Performance Status* widget, mousing over the scatter chart displays the status for health checks and member interface in a tooltip. The colors (red, orange, yellow, and green) indicate the different percentage of a member's interface or health check.

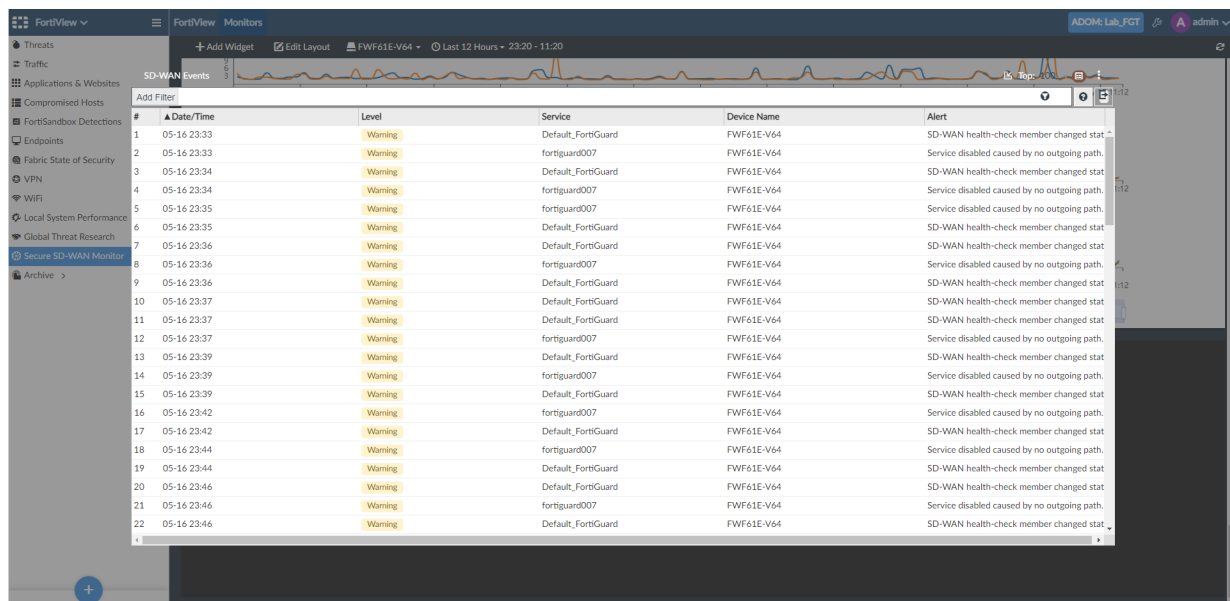




In the *SD-WAN Performance Status* widget, click on a scatter chart to view additional details.



The *SD-WAN High and Critical Events* widget has been replaced with the new *SD-WAN Events* widget. This widget displays a table chart for SD-WAN event logs which have a level higher than notice (warning, error, etc.) within the selected time period.



# Security Operations (SOC)

This section lists the new features added to FortiAnalyzer for security operations (SOC):

- [SOC automation on page 15](#)
- [Incident and Event Management on page 31](#)
- [Dashboards on page 39](#)

## SOC automation

This section lists the new features added to FortiAnalyzer for SOC automation:

- [FortiOS connector health check on page 15](#)
- [Attach FortiMail connector actions to incidents on page 18](#)
- [SIEM correlation and analysis on page 23](#)
- [Importing and exporting playbooks on page 25](#)
- [FortiGuard outbreak and alert service on page 26](#)
- [Manage subnets on page 30](#)

### FortiOS connector health check

This enhanced feature provides visibility on the FortiOS connectors status.

**To view the status of FortiOS connectors:**

1. Go to *FortiSoC > Automation > Connectors*, and click the FortiOS connector to expand the list and display all FortiGate devices.

The screenshot shows the FortiSoC interface with the 'Connectors' section selected in the left sidebar. The main panel displays a list of connectors under the 'FOS connectors' tab. The connectors are organized into three sections: 'FOS - FortiOS Connector', 'FGT-VM-64', and 'Shawn-CSF'. Each section contains a table of automation rules, actions, and parameters.

| Automation Rule              | Automation Action(s)        | Parameters |
|------------------------------|-----------------------------|------------|
| trigger_add_cnc_to_blacklist | action_add_cnc_to_blacklist | cncip      |
| trigger_activate_strict_ips  | action_activate_strict_ips  | policyid   |


  

| Automation Rule              | Automation Action(s)                                                                         | Parameters  |
|------------------------------|----------------------------------------------------------------------------------------------|-------------|
| trigger_add_cnc_to_blacklist | action_add_cnc_to_blacklist                                                                  | cncip       |
| activate_strict_ips          | activate_strict_ips_shawn<br>activate_strict_ips                                             | policyid    |
| add_cnc_to_blacklist         | add_cnc_to_blacklist                                                                         | cncip       |
| Incoming Webhook Quarantine  | Incoming Webhook Quarantine_quarantine-forticlient<br>Incoming Webhook Quarantine_quarantine | uuid<br>mac |
| trigger_activate_strict_ips  | action_activate_strict_ips                                                                   | policyid    |




  




| Automation Rule              | Automation Action(s)                                                                         | Parameters  |
|------------------------------|----------------------------------------------------------------------------------------------|-------------|
| add_cnc_to_blacklist         | add_cnc_to_blacklist                                                                         | cncip       |
| Trigger_activate_strict_ips  | Action_activate_strict_ips                                                                   | policyid    |
| Trigger_add_cnc_to_blacklist | Action_add_cnc_to_blacklist                                                                  | cncip       |
| Incoming Webhook Quarantine  | Incoming Webhook Quarantine_quarantine-forticlient<br>Incoming Webhook Quarantine_quarantine | uuid<br>mac |
| activate_strict_ips          | activate_strict_ips_shawn                                                                    | policyid    |

Devices are organized by standalone, Cooperative Security Fabric (CSF), and high availability (HA). Clicking a CSF or HA grouping will expand the list to display all FortiGate members.

 FOS - FortiOS Connector

Actions








| Automation Rule              | Automation Action(s)        | Parameters |
|------------------------------|-----------------------------|------------|
| trigger_add_cnc_to_blacklist | action_add_cnc_to_blacklist | cncip      |
| trigger_activate_strict_ips  | action_activate_strict_ips  | policyid   |

| Automation Rule              | Automation Action(s)                                                                         | Parameters  |
|------------------------------|----------------------------------------------------------------------------------------------|-------------|
| add_cnc_to_blacklist         | add_cnc_to_blacklist                                                                         | cncip       |
| Trigger_activate_strict_ips  | Action_activate_strict_ips                                                                   | policyid    |
| Trigger_add_cnc_to_blacklist | Action_add_cnc_to_blacklist                                                                  | cncip       |
| Incoming Webhook Quarantine  | Incoming Webhook Quarantine_quarantine-forticlient<br>Incoming Webhook Quarantine_quarantine | uuid<br>mac |
| activate_strict_ips          | activate_strict_ips_shawn<br>activate_strict_ips                                             | policyid    |

Status icons in green indicate the API connection is up. Status icons in red indicate the API connection is down. You can hover your mouse over a status icon to see the last active time.

 FOS - FortiOS Connector

Actions

API connection is successful, (last active at 2020/11/26 13:25:11)

| Automation Rule              | Automation Action(s)        | Parameters |
|------------------------------|-----------------------------|------------|
| trigger_add_cnc_to_blacklist | action_add_cnc_to_blacklist | cncip      |
| trigger_activate_strict_ips  | action_activate_strict_ips  | policyid   |

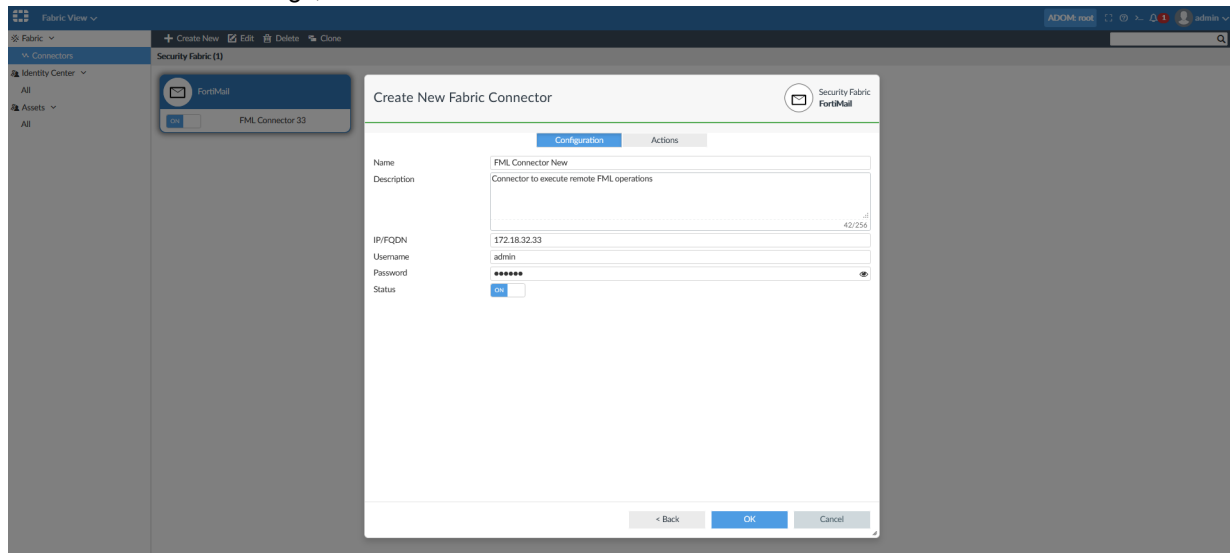
Click the refresh icon to get an updated connector status.

## Attach FortiMail connector actions to incidents

This feature will help users to see the result of FortiMail playbook actions in the incident analysis page. Information can be found within the *Indicators* tab of the incident analysis page once added.

### To use the action in a FortiSoC playbook:

1. Go to *Fabric View*. Click *Create New* and choose *FortiMail* under the *Security Fabric* category. Configure the FortiMail connector settings, and click *OK*.



2. Create a playbook to get email statistics and attach the data to an incident.  
Go to *FortiSoC > Automation > Playbook*, and create a new playbook from scratch. In this example, the playbook is called *GetMailStats*.

- a. Select the *On\_Demand* trigger as the starter.
- b. Create a task using the FortiMail connector with the *Get Email Statistics* action.

The screenshot shows the FortiAnalyzer interface for configuring a playbook named 'GetMailStats'. The left sidebar contains navigation options like Dashboards, Playbooks, Incidents, Events, Automation, Connectors, and Playbook Monitor. The main canvas displays a workflow diagram with three steps: 1. ON\_DEMAND STARTER, 2. GET\_EMAIL\_STATISTICS (labeled 'GetStatus'), and 3. ATTACH\_DATA\_TO\_INCIDENT (labeled 'Attach'). The right-hand configuration panel for 'FML\_GET\_EMAIL\_STATISTICS' includes fields for Name (GetStatus), Description, Connector (FML Connector New), Action (Get Email Statistics), email (Playbook Starter), and Time Range (This Week). At the bottom of the canvas are 'Save Playbook' and 'Cancel' buttons.

- c. Create a second task using the local connector with the *Attach Data to Incident* action.

This screenshot shows the same 'GetMailStats' playbook configuration, but with the second task updated. The workflow diagram remains the same. The right-hand configuration panel is now for 'LOCALHOST\_ATTACH\_DATA\_TO\_INCIDENT'. It shows Name: Attach, Connector: Local Connector, Action: Attach Data to Incident, Incident ID: IN00000001, and Attachment: GetStatus (id\_1ef\_8c9\_9\_...). The 'Save Playbook' and 'Cancel' buttons are still at the bottom.

- d. Click *OK* to save the playbook.
3. Create a second playbook to get the sender reputation and attach the data to an incident. In this example, the playbook is called *GetSenderReputation*.

- a. Select the *On\_Demand* trigger as the starter.
- b. Create a task using the FortiMail connector with the *Get Sender Reputation* action.

The screenshot shows the FortiAnalyzer GUI with the 'GetSenderReputation' playbook being configured. The left sidebar shows the navigation menu with 'Playbook' selected. The main canvas displays a flowchart with three steps: 'ON\_DEMAND STARTER', 'GET\_SENDER\_REPUTATION (GetReputation)', and 'ATTACH\_DATA\_TO\_INCIDENT (AttachIncident)'. The right panel, titled 'FML\_GET\_SENDER\_REPUTATION', contains the configuration for the 'GET\_SENDER\_REPUTATION' step. It shows the connector set to 'FML Connector New' and the action set to 'Get Sender Reputation'. The 'ip' field is populated with '172.16.81.1'. The 'Save Playbook' button is visible at the bottom of the canvas.

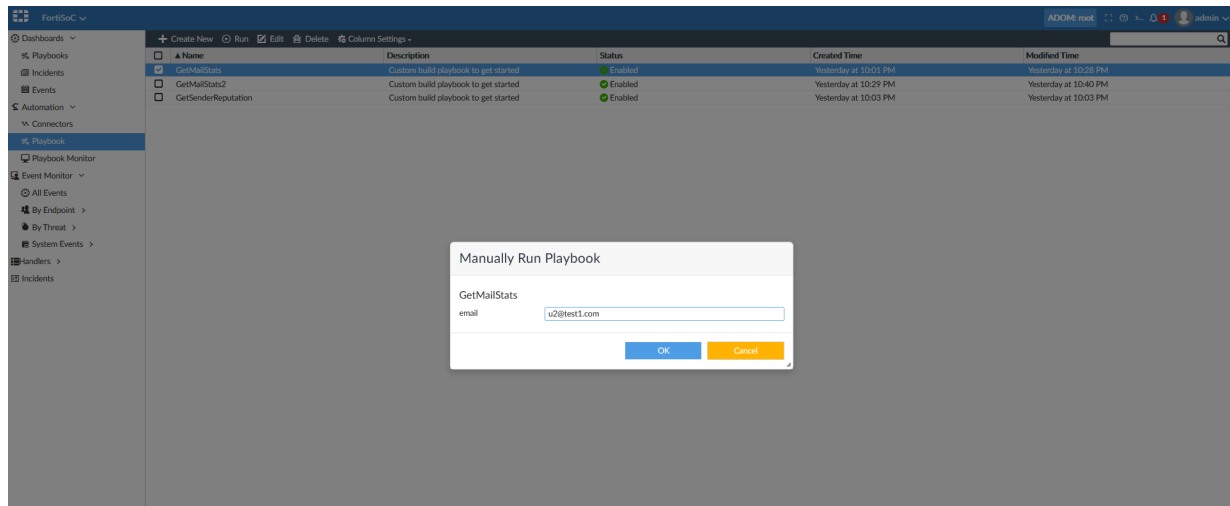
- c. Create a second task using the local connector with the *Attach Data to Incident* action.

The screenshot shows the FortiAnalyzer GUI with the 'GetSenderReputation' playbook being configured. The left sidebar shows the navigation menu with 'Playbook' selected. The main canvas displays a flowchart with three steps: 'ON\_DEMAND STARTER', 'GET\_SENDER\_REPUTATION (GetReputation)', and 'ATTACH\_DATA\_TO\_INCIDENT (AttachIncident)'. The right panel, titled 'LOCALHOST\_ATTACH\_DATA\_TO\_INCIDENT', contains the configuration for the 'ATTACH\_DATA\_TO\_INCIDENT' step. It shows the connector set to 'Local Connector' and the action set to 'Attach Data to Incident'. The 'Incident ID' field is populated with 'INC0000001' and the 'Attachment' field is populated with 'GetReputation (id\_265\_8... reputation)'. The 'Save Playbook' button is visible at the bottom of the canvas.

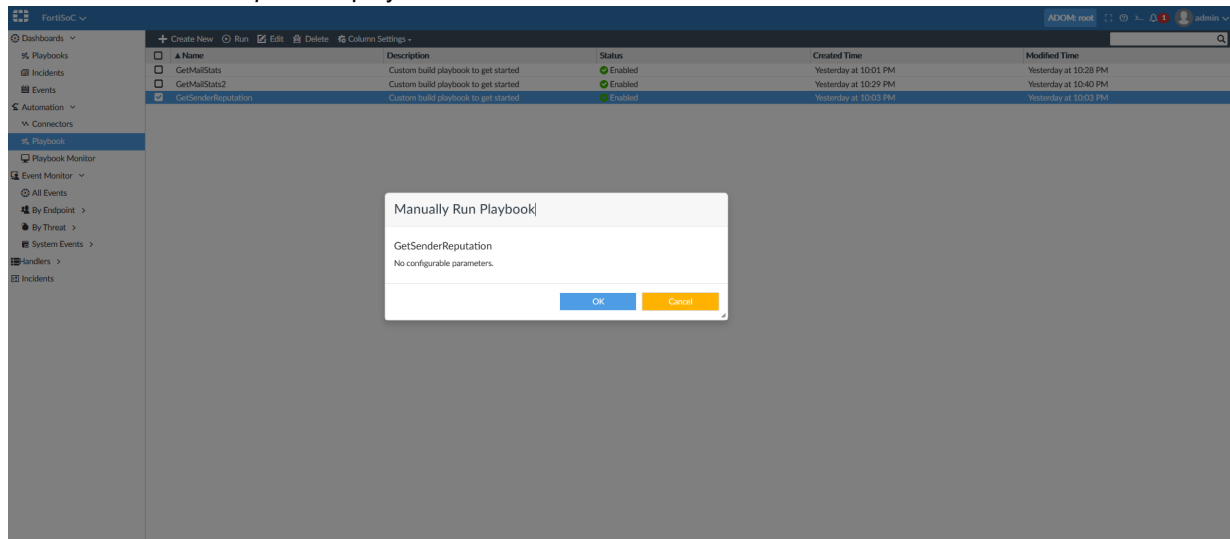
- d. Click *OK* to save the playbook.



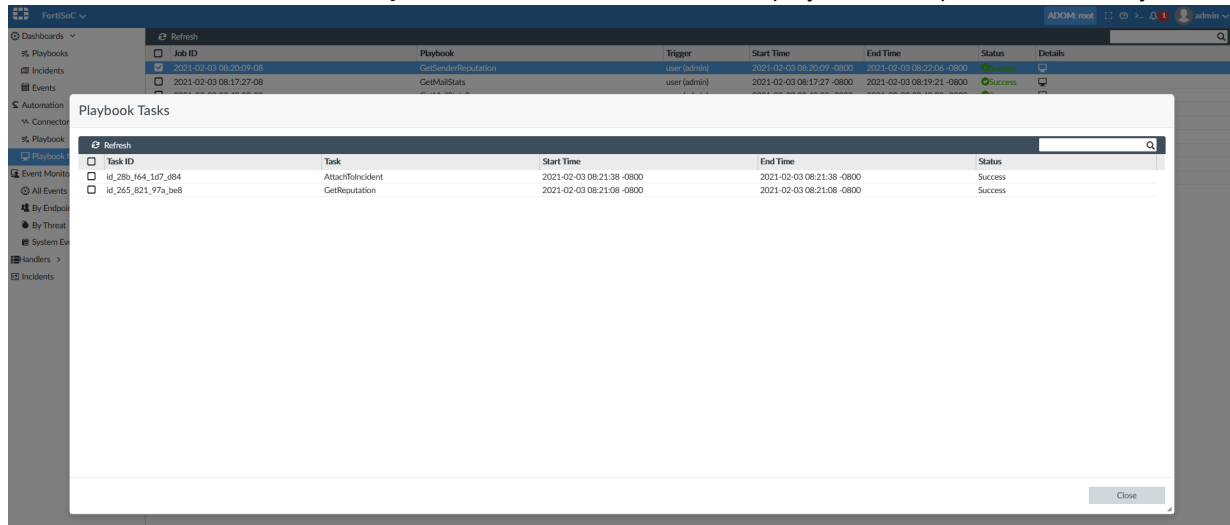
4. Run the *GetMailStats* playbook to retrieve statistics for the provided email address. This example uses `u2@test1.com`.



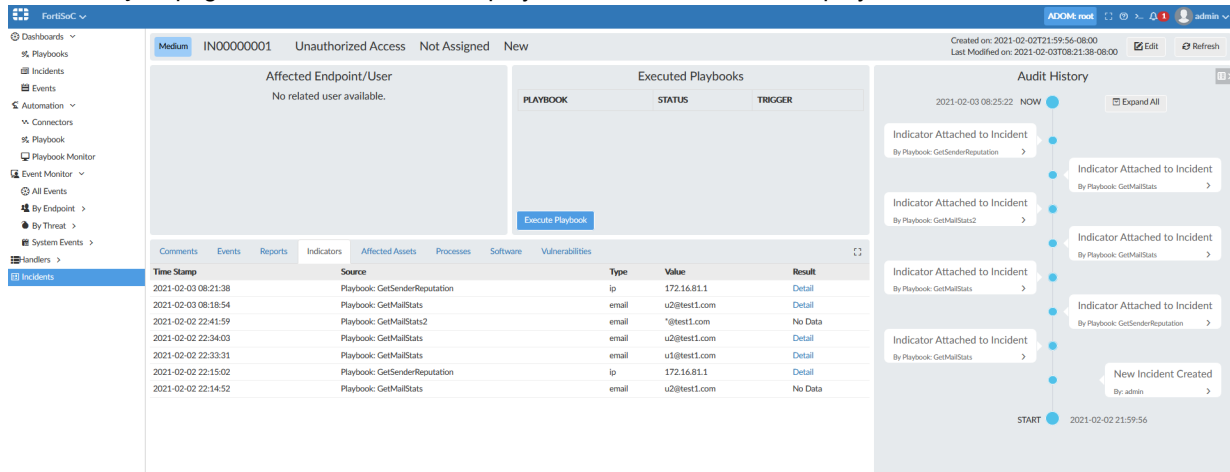
5. Run the *GetSenderReputation* playbook.



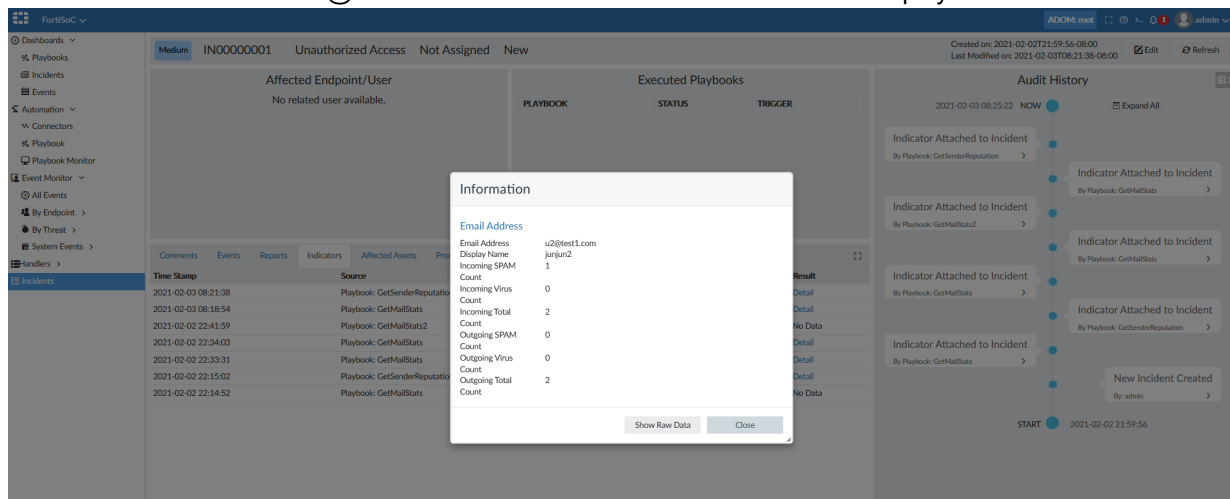
6. Go to **FortiSoC > Automation > Playbook Monitor** to confirm that both playbooks completed successfully.



7. Go to **FortiSoC > Incidents**. Right-click on the selected incident and select **Analysis**. In the **Analysis** page, select **Indicators**. The playbook action results are displayed.



Click on the details for the **u2@test1** email address. The detailed statistics are displayed.



Click on the details for the 172.16.81.1 address. The detailed reputation is displayed.

The screenshot shows the FortiSoC interface with a table of events. An 'Information' pop-up window is open, displaying details for the Network Address 172.16.81.1. The details include:

- Address: 172.16.81.1
- Score: 0
- State: score controlled
- Client CC: ZZ
- Last Modified: Jun 22, 2020 12:00:00 PM
- Client Location: Reserved

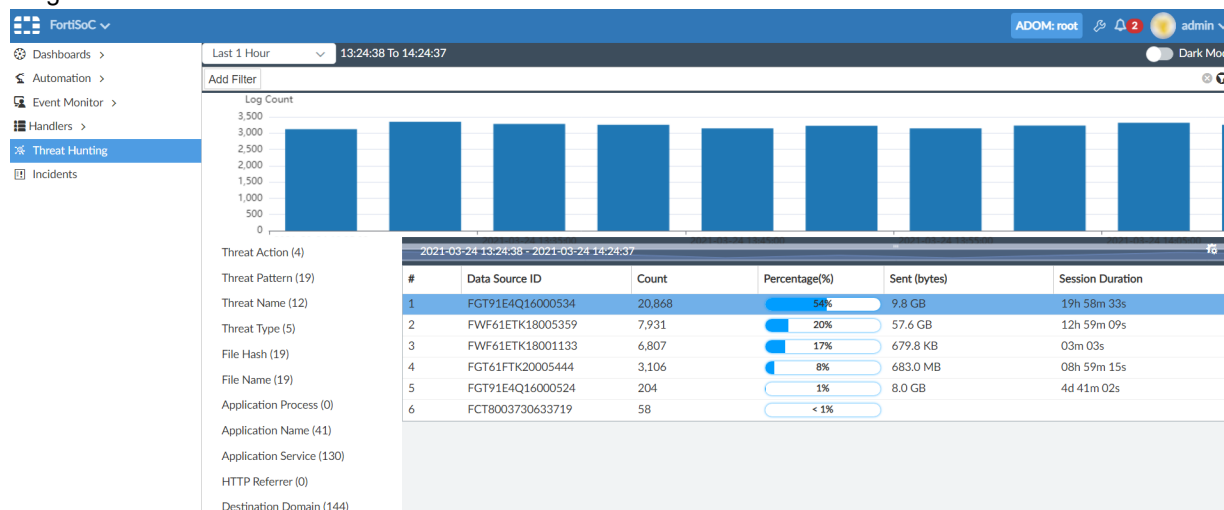
## SIEM correlation and analysis

Expand the built-in SIEM framework for automated correlation and analysis using the normalized log fields that are critical for SOC threat hunting. Data is aggregated, correlated across these interesting log fields, and organized in a digestible format ready for SOC to consume. Global filters can be applied on the fly to help the SOC quickly zero into the interesting timeline, endpoint events, and suspicious activities, identify anomalies and behavior patterns and uncover hidden threats.

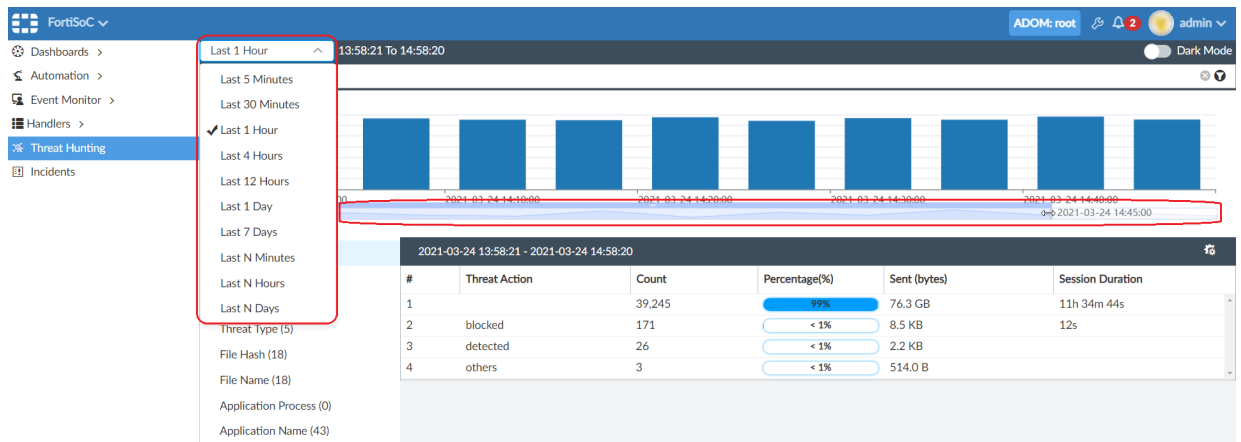
### To view the Threat Hunting dashboard:

#### 1. Go to *FortiSoC > Threat Hunting*.

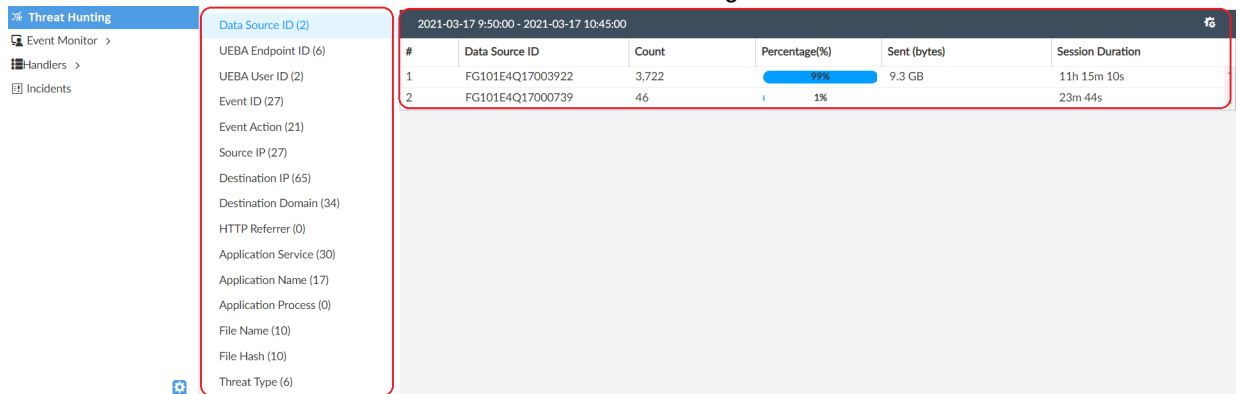
The *Threat Hunting* dashboard is displayed. This dashboard provides fast searching (drilldown) with cached data on fields of interest based on the SIEM database and includes a graphical chart for Log Count during the specified time range.



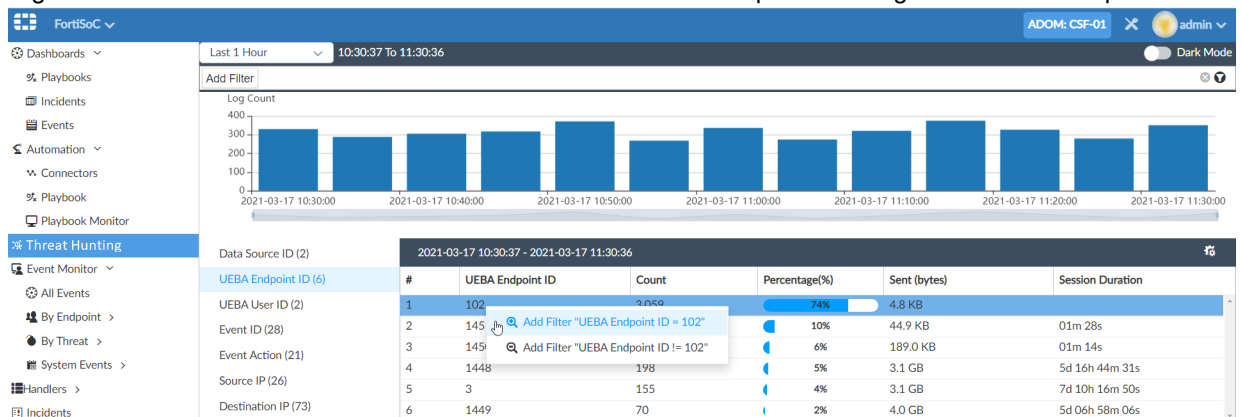
The dashboard includes a predefined time filter to specify the time range you want to view. You can manually drag the progress bar below the *Log Count* graph to display the chart in different time ranges, and the data will change accordingly.



The left pane includes a list of selectable fields of interest. The right pane provides analytics to display the actual values for the selected field with statistics in the selected time range.



## 2. Right-click on a value in the table to add it to a filter. Fields in the left pane and Log Count chart are updated.



- Double-click a column of interest on the right pane to drilldown and see detailed log information. The drilldown view provides the same functions as Log View, including a search bar filter, time filter, columns setting.

The screenshot shows the Threat Hunting interface with a list of events. A context menu is open over the 'Event Type' column, showing options to 'Add Filter' with the filter 'Event Type = traffic'.

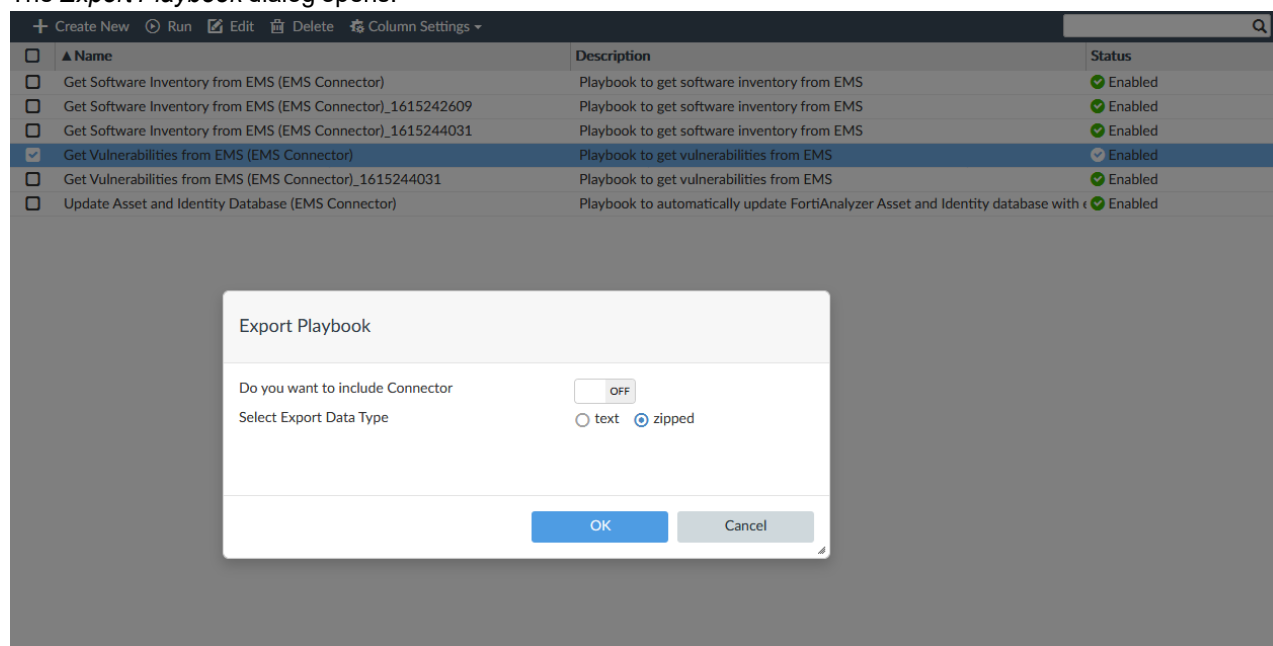
| #  | Date/Time | Data Source ID   | Event Message      | Event Type | Event Severity | Source IP        | Destination IP | Host Name     | User ID | Application N... |
|----|-----------|------------------|--------------------|------------|----------------|------------------|----------------|---------------|---------|------------------|
| 1  | 11:30:35  | FG101E4Q17003922 |                    | traffic    | notice         | fe80::d579:8f... | ff02::1:2      |               |         | DHCP6            |
| 2  | 11:30:35  | FG101E4Q17003922 |                    | traffic    | notice         | 0.0.0.0          | 255.255.255... |               |         | DHCP/DHCP ...    |
| 3  | 11:30:35  | FG101E4Q17003922 |                    | traffic    | notice         | 0.0.0.0          | 255.255.255... |               |         | DHCP/DHCP ...    |
| 4  | 11:30:30  | FG101E4Q17003922 |                    | traffic    | notice         | 192.168.1.119    | 10.2.60.103    | 192.168.1.119 |         |                  |
| 5  | 11:30:30  | FG101E4Q17003922 | A rating error ... | utm        | notice         | 11               | 211.152.146.73 | 10.2.60.111   |         |                  |
| 6  | 11:30:30  | FG101E4Q17003922 | Social Media: ...  | utm        | notice         | 11               | 211.152.146.73 | 10.2.60.111   |         | Sohu             |
| 7  | 11:30:30  | FG101E4Q17003922 |                    | traffic    | notice         | 0.0.0.0          | 255.255.255... |               |         | DHCP/DHCP ...    |
| 8  | 11:30:30  | FG101E4Q17003922 | System perfor...   | event      | notice         |                  |                |               |         |                  |
| 9  | 11:30:28  | FG101E4Q17003922 |                    | traffic    | notice         | 0.0.0.0          | 255.255.255... |               |         | DHCP/DHCP ...    |
| 10 | 11:30:28  | FG101E4Q17003922 | Domain is mo...    | utm        | notice         | 10.2.60.111      | 172.17.254.151 | 10.2.60.111   |         |                  |
| 11 | 11:30:28  | FG101E4Q17003922 | Domain is mo...    | utm        | notice         | 10.2.60.111      | 172.17.254.151 | 10.2.60.111   |         |                  |
| 12 | 11:30:28  | FG101E4Q17003922 |                    | utm        | information    | 10.2.60.111      | 172.17.254.151 | 10.2.60.111   |         |                  |
| 13 | 11:30:28  | FG101E4Q17003922 |                    | utm        | information    | 10.2.60.111      | 172.17.254.151 | 10.2.60.111   |         |                  |
| 14 | 11:30:28  | FG101E4Q17003922 |                    | traffic    | notice         | fe80::d579:8f... | ff02::1:2      |               |         | DHCP6            |
| 15 | 11:30:25  | FG101E4Q17003922 |                    | traffic    | notice         | 0.0.0.0          | 255.255.255... |               |         | DHCP/DHCP ...    |

## Importing and exporting playbooks

This feature adds the ability to import/export playbooks with the option to include connector data.

### To export a playbook:

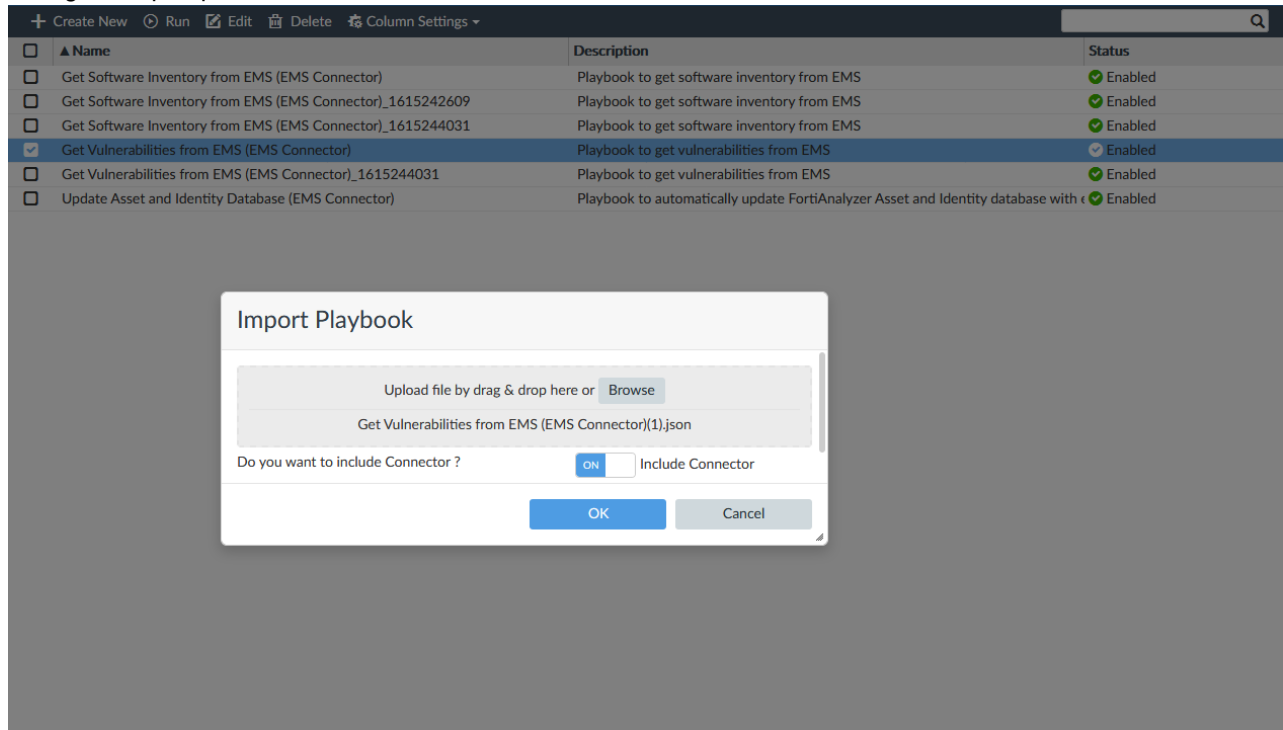
- Go to *FortiSoC > Automation > Playbook*.
- Highlight the playbook(s) that you want to export, then right-click in the dashboard and click *Export*. The *Export Playbook* dialog opens.



- Configure the settings for exporting the selected playbook:
  - Do you want to include Connector:** When enabled, connector configurations required to run this playbook will be included in the exported file.
  - Select Export Data Type:** Select the export file type as either plain text JSON or zipped/base 64 encoded JSON.
- Click **OK**. The file will be downloaded locally and is viewable within another editor when in the plain text format.

**To import a playbook:**

1. Go to *FortiSoC > Automation > Playbook* in another FortiAnalyzer ADOM.
2. Right-click in the playbook dashboard, and click *Import*.  
The *Import Playbook* dialog appears.
3. Click *Browse* and select the playbook file to be imported. .  
When the playbook file includes connectors, you will see a toggle allowing you to include or exclude the connectors during the import process.



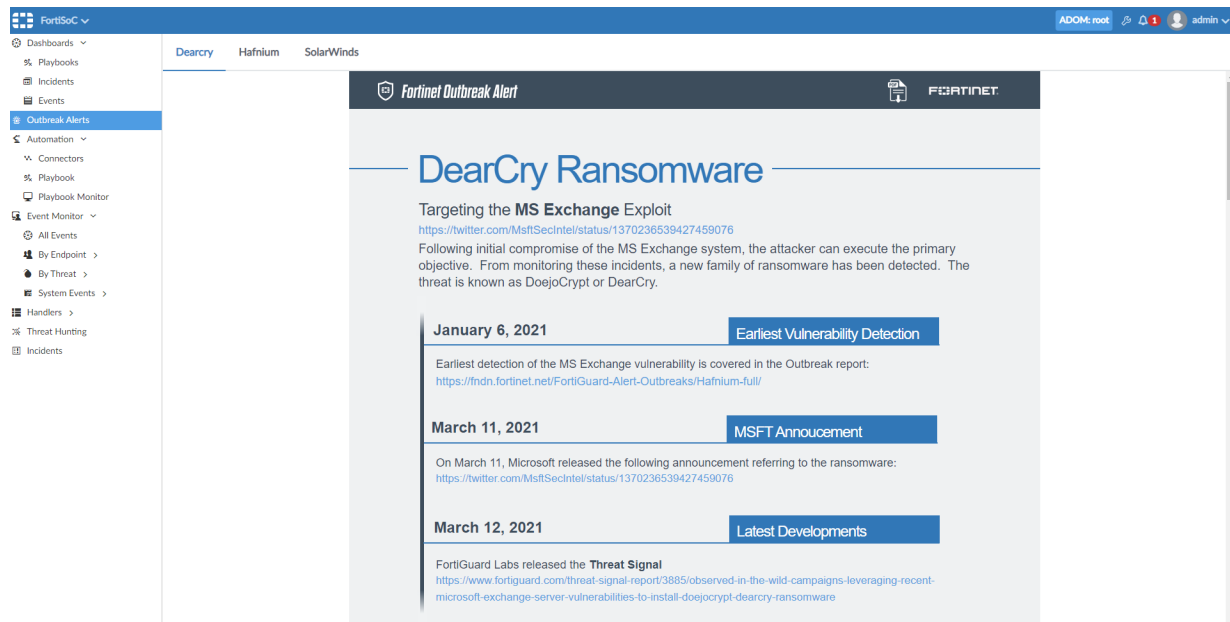
4. Click *OK*. A message is displayed to confirm that the playbook was imported successfully.  
When a playbook or connector being imported shares the same name as an existing one, a new name will be created which includes the timestamp. Playbooks will be automatically updated with the new connector name.

**FortiGuard outbreak and alert service**

A new FortiGuard Outbreak Alert Service (FOAS) is now available through the Enterprise Protection bundle to protect customer's networks against malware outbreaks. The Outbreak Alert content package consists of a FortiGuard Report for the outbreak, an Event Handler, and a Report Template to detect the outbreak.

**To view outbreak alerts, reports, and event handlers:**

1. Go to *FortiSoC > Outbreak Alerts*. Available outbreak alerts, including DearCry, Hafnium, and SolarWinds, are displayed and can be browsed in all ADOMs.  
The outbreak alert can be downloaded by clicking on the download icon.



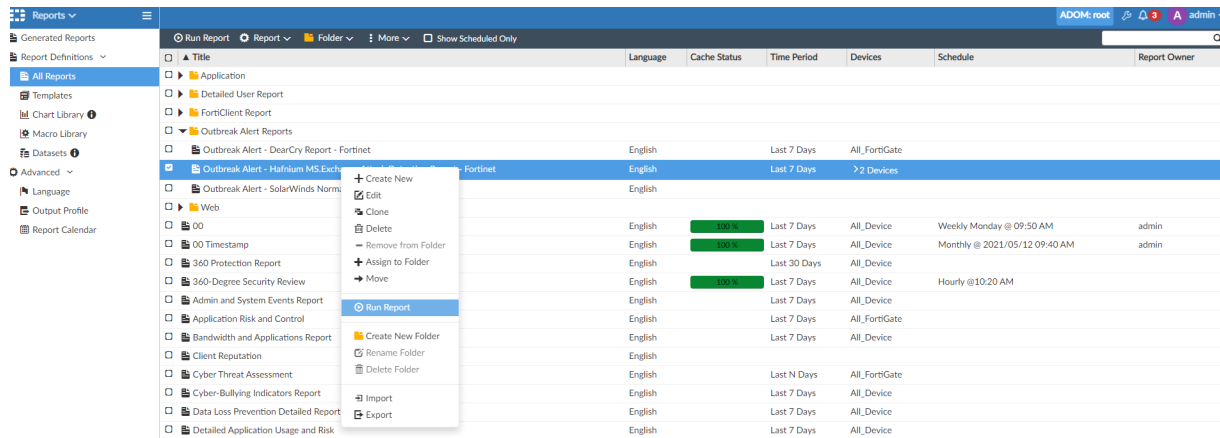
2. Go to **FortiSoC > Handlers > Event Handler List**. Corresponding outbreak alert event handlers are installed and listed in related ADOMs automatically.

| Status | Name                                                             | Filters      | Devices      | Send Alert to | Events | Included Subnets | Excluded Subnets |
|--------|------------------------------------------------------------------|--------------|--------------|---------------|--------|------------------|------------------|
| ✓      | Local Device Event                                               | > 1 Filter   | Local Device |               | 189    |                  |                  |
| ✓      | Default-Botnet-Communication-Detection-By-Threat                 | > 9 Filters  | All Devices  |               |        |                  |                  |
| ✓      | Default-Compromised Host-Detection-IOC-By-Threat                 | > 3 Filters  | All Devices  |               |        |                  |                  |
| ✓      | Default-Malicious-Code-Detection-By-Threat                       | > 8 Filters  | All Devices  |               | 1891   |                  |                  |
| ✓      | Default-Risky-Destination-Detection-By-Threat                    | > 15 Filters | All Devices  |               | 1084   |                  |                  |
| ✓      | Default-Risky-App-Detection-By-Threat                            | > 2 Filters  | All Devices  |               | 270    |                  |                  |
| ✓      | Default-Malicious-File-Detection-By-Threat                       | > 8 Filters  | All Devices  |               | 2      |                  |                  |
| ✓      | Default-Risky-App-Detection-By-Endpoint                          | > 4 Filters  | All Devices  |               | 270    |                  |                  |
| ✓      | Default-Malicious-File-Detection-By-Endpoint                     | > 24 Filters | All Devices  |               | 2      |                  |                  |
| ✓      | Default-Malicious-Code-Detection-By-Endpoint                     | > 8 Filters  | All Devices  |               | 1889   |                  |                  |
| ✓      | Default-Risky-Destination-Detection-By-Endpoint                  | > 14 Filters | All Devices  |               | 375    |                  |                  |
| ✓      | Default-Compromised Host-Detection-IOC-By-Endpoint               | > 3 Filters  | All Devices  |               |        |                  |                  |
| ✓      | Default-Botnet-Communication-Detection-By-Endpoint               | > 9 Filters  | All Devices  |               |        |                  |                  |
| ✓      | Outbreak Alert - Fortinet_SOC-Hafnium-MS-Exchange-Attack-Detect  | > 4 Filters  | All Devices  |               |        |                  |                  |
| ✓      | Outbreak Alert - Fortinet_SOC-Deary-Ransomware-Detection         | > 3 Filters  | All Devices  |               |        |                  |                  |
| ✓      | Outbreak Alert - Fortinet_SOC-Compromised Host Detection. SolarW | > 18 Filters | All Devices  |               |        |                  |                  |
| ✗      | Default-FFW System Events                                        | > 8 Filters  | All Devices  |               |        |                  |                  |
| ✗      | Default-FFW-Compromised Host-Detection-IOC-By-Threat             | > 3 Filters  | All Devices  |               |        |                  |                  |
| ✗      | Default-FFW-Risky-Destination-Detection-By-Threat                | > 10 Filters | All Devices  |               |        |                  |                  |
| ✗      | Default-FFW-Risky-Destination-Detection-By-Endpoint              | > 10 Filters | All Devices  |               |        |                  |                  |
| ✗      | Default-FFW-Compromised Host-Detection-IOC-By-Endpoint           | > 2 Filters  | All Devices  |               |        |                  |                  |
| ✗      | Default-FFW-Botnet-Communication-Detection-By-Endpoint           | > 1 Filter   | All Devices  |               |        |                  |                  |
| ✗      | Default-FFW-Threat-Detection-By-Hostname                         | > 4 Filters  | All Devices  |               |        |                  |                  |

3. Go to **Reports > Report Definitions > All Reports**.

A new **Outbreak Alert Reports** folder is available in all ADOMs. All outbreak reports are stored in this folder. Current outbreak reports include **DearCry Report**, **Hafnium M.S.Exchange Attack Detection Report**, and **SolarWinds Normalized Report**, available in Fabric ADOMs.

Right click a report to run the report. Reports can be generated in HTML, PDF, XML, and CSV formats.



Below is an example of the *Hafnium M.S.Exchange Attack Detection Report*.

#### Summary

This report displays the findings on attack attempts to exploit MS. Exchange vulnerabilities from Fortigate.

This table shows detections by FortiGate IPS:

#### FortiGate IPS Detection

| # | Device                | Source         | Destination     | Attack                                            | Total Count | First Seen          | Last Seen           |
|---|-----------------------|----------------|-----------------|---------------------------------------------------|-------------|---------------------|---------------------|
| 1 | Van_Office_FW1_Master | 172.16.68.21   | 111.206.21.0.75 | HTTP.Unknown.Tunnelling                           | 3           | 2021-04-13 18:12:50 | 2021-04-13 20:44:44 |
| 2 | Van_Office_FW1_Master | 172.18.34.21   | 74.125.124.94   | TCP.PORT0                                         | 3           | 2021-04-13 18:12:50 | 2021-04-13 20:44:44 |
| 3 | Van_Office_FW1_Master | 172.16.197.102 | 10.50.0.0       | TCP.PORT0                                         | 3           | 2021-04-13 18:12:50 | 2021-04-13 20:44:44 |
| 4 | Van_Office_FW1_Master | 172.16.171.64  | 172.18.22.4     | MS.Exchange.Server.UM.Core.Remote.Co de.Execution | 3           | 2021-04-13 18:12:50 | 2021-04-13 20:44:44 |
| 5 | FGT91E4Q16000534      | 172.16.68.21   | 111.206.21.0.75 | HTTP.Unknown.Tunnelling                           | 1           | 2021-04-13 18:15:19 | 2021-04-13 18:15:19 |
| 6 | FGT91E4Q16000534      | 172.16.171.64  | 172.18.22.4     | MS.Exchange.Server.UM.Core.Remote.Co de.Execution | 1           | 2021-04-13 18:15:19 | 2021-04-13 18:15:19 |
| 7 | FGT91E4Q16000534      | 172.18.34.21   | 74.125.124.94   | TCP.PORT0                                         | 1           | 2021-04-13 18:15:19 | 2021-04-13 18:15:19 |
| 8 | FGT91E4Q16000534      | 172.16.197.102 | 10.50.0.0       | TCP.PORT0                                         | 1           | 2021-04-13 18:15:19 | 2021-04-13 18:15:19 |

This table shows detections by FortiGate AV:

#### FortiGate AV Detection

| # | Device                | Source      | Destination  | Virus             | Total Count | First Seen          | Last Seen           |
|---|-----------------------|-------------|--------------|-------------------|-------------|---------------------|---------------------|
| 1 | Van_Office_FW1_Master | 10.2.60.143 | 10.2.175.110 | HTML/Agent.A121tr | 1           | 2021-04-13 20:44:55 | 2021-04-13 20:44:55 |
| 2 | Van_Office_FW1_Master | 10.2.60.143 | 10.2.175.110 | ASP/WebShell.cltr | 1           | 2021-04-13 20:44:55 | 2021-04-13 20:44:55 |

- When FortiAnalyzer does not have a valid FOAS license, a default Fortinet Outbreak Alert page is displayed with a reminder that to get outbreak alert services, you need a license. The option to download outbreak alerts is not



available until you have a valid license.

**Fortinet Outbreak Alert**

To get outbreak alert service, you need to get a license online.

# SolarWinds

In the Wild since March/2020

<https://us-cert.cisa.gov/ncas/alerts/aa20-352a>  
<https://www.solarwinds.com/securityadvisory/faq>

Solarwinds [signed] software containing a planted vulnerability released in March 2020 as a regular (trusted) software patch. The backdoor was not discovered until the FireEye breach became public 9 months later.

**Pre-March/2020** **Supply Chain Attack**

SolarWinds was the victim of a complex & targeted supply chain cyber attack, with the primary goal of inserting a malicious backdoor into trusted (signed) software, which could later be exploited in end-customer installations of the SolarWinds Orion platform. As reported by SolarWinds, the earliest visible account of the attacker shows test code inserted in the October, 2019 software release.

<https://www.solarwinds.com/securityadvisory>

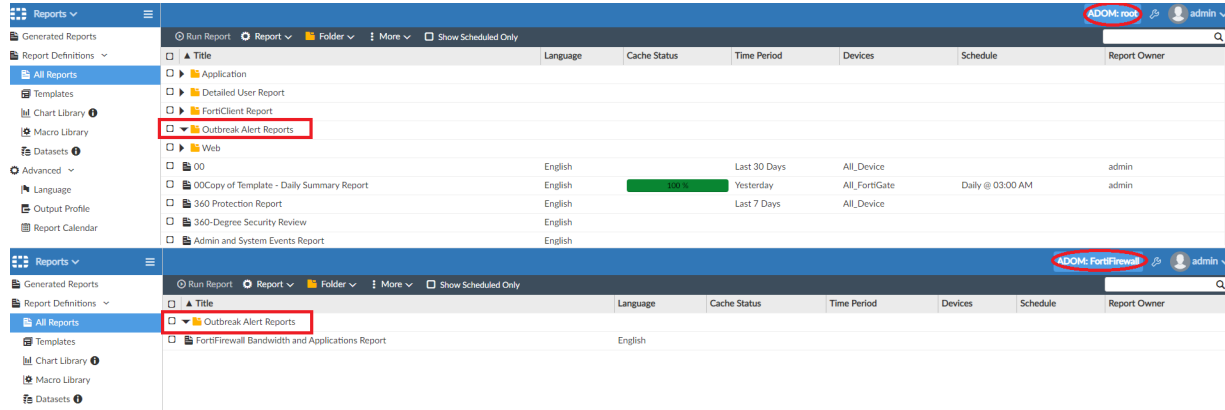
## 5. Go to FortiSOc > Handlers > Event Handler List.

Without a valid license, no outbreak related event handlers are available.

| Status                                                 | Name                                                   | Filters      | Devices      | Send Alert to | Events | Included Subnets | Excluded Subnets |
|--------------------------------------------------------|--------------------------------------------------------|--------------|--------------|---------------|--------|------------------|------------------|
| Local Device Event                                     | Local Device Event                                     | > 1 Filter   | Local Device |               | 160    |                  |                  |
| Default-Botnet-Communication-Detection-By-Threat       | Default-Botnet-Communication-Detection-By-Threat       | > 9 Filters  | All Devices  |               |        |                  |                  |
| Default-Compromised-Host-Detection-IOC-By-Threat       | Default-Compromised-Host-Detection-IOC-By-Threat       | > 3 Filters  | All Devices  |               |        |                  |                  |
| Default-Malicious-Code-Detection-By-Threat             | Default-Malicious-Code-Detection-By-Threat             | > 8 Filters  | All Devices  |               | 3316   |                  |                  |
| Default-Risky-Destination-Detection-By-Threat          | Default-Risky-Destination-Detection-By-Threat          | > 15 Filters | All Devices  |               | 1886   |                  |                  |
| Default-Risky-App-Detection-By-Threat                  | Default-Risky-App-Detection-By-Threat                  | > 2 Filters  | All Devices  |               | 338    |                  |                  |
| Default-Malicious-File-Detection-By-Threat             | Default-Malicious-File-Detection-By-Threat             | > 8 Filters  | All Devices  |               |        |                  |                  |
| Default-Risky-App-Detection-By-Endpoint                | Default-Risky-App-Detection-By-Endpoint                | > 4 Filters  | All Devices  |               | 338    |                  |                  |
| Default-Malicious-File-Detection-By-Endpoint           | Default-Malicious-File-Detection-By-Endpoint           | > 24 Filters | All Devices  |               |        |                  |                  |
| Default-Malicious-Code-Detection-By-Endpoint           | Default-Malicious-Code-Detection-By-Endpoint           | > 8 Filters  | All Devices  |               | 3312   |                  |                  |
| Default-Risky-Destination-Detection-By-Endpoint        | Default-Risky-Destination-Detection-By-Endpoint        | > 14 Filters | All Devices  |               | 737    |                  |                  |
| Default-Compromised-Host-Detection-IOC-By-Endpoint     | Default-Compromised-Host-Detection-IOC-By-Endpoint     | > 3 Filters  | All Devices  |               |        |                  |                  |
| Default-Botnet-Communication-Detection-By-Endpoint     | Default-Botnet-Communication-Detection-By-Endpoint     | > 9 Filters  | All Devices  |               |        |                  |                  |
| Default-FFW-System-Events                              | Default-FFW-System-Events                              | > 8 Filters  | All Devices  |               |        |                  |                  |
| Default-FFW-Compromised-Host-Detection-IOC-By-Threat   | Default-FFW-Compromised-Host-Detection-IOC-By-Threat   | > 3 Filters  | All Devices  |               |        |                  |                  |
| Default-FFW-Destination-Detection-By-Threat            | Default-FFW-Destination-Detection-By-Threat            | > 10 Filters | All Devices  |               |        |                  |                  |
| Default-FFW-Risky-Destination-Detection-By-Endpoint    | Default-FFW-Risky-Destination-Detection-By-Endpoint    | > 10 Filters | All Devices  |               |        |                  |                  |
| Default-FFW-Compromised-Host-Detection-IOC-By-Endpoint | Default-FFW-Compromised-Host-Detection-IOC-By-Endpoint | > 2 Filters  | All Devices  |               |        |                  |                  |
| Default-FFW-Botnet-Communication-Detection-By-Endpoint | Default-FFW-Botnet-Communication-Detection-By-Endpoint | > 1 Filter   | All Devices  |               |        |                  |                  |
| Default-FWB-Threat-Detection-By-Hostname               | Default-FWB-Threat-Detection-By-Hostname               | > 4 Filters  | All Devices  |               |        |                  |                  |
| Default-FDC-Honey-Pot-Detection                        | Default-FDC-Honey-Pot-Detection                        | > 1 Filter   | All Devices  |               |        |                  |                  |
| Default-FCT-Threat-Detection-By-Threat                 | Default-FCT-Threat-Detection-By-Threat                 | > 2 Filters  | All Devices  |               |        |                  |                  |
| Default-FCT-Threat-Detection-By-Endpoint               | Default-FCT-Threat-Detection-By-Endpoint               | > 3 Filters  | All Devices  |               |        |                  |                  |
| Default-FSA-Malware-Handler-By-Threat                  | Default-FSA-Malware-Handler-By-Threat                  | > 6 Filters  | All Devices  |               |        |                  |                  |
| Default-FSA-Malware-Handler-By-Endpoint                | Default-FSA-Malware-Handler-By-Endpoint                | > 4 Filters  | All Devices  |               |        |                  |                  |

## 6. Go to *Reports > Report Definitions > All Reports*.

Without a valid license, the new *Outbreak Alerts Reports* folder is displayed, but no reports are assigned to it.



## To configure FortiGuard settings in the CLI:

### 1. In the FortiAnalyzer CLI, enter the following command:

```
config fmupdate fds-setting
(fds-setting) # show
config fmupdate fds-setting
config server-override
set status enable
config servlist
edit 1
set ip 192.168.X.X
```

## Manage subnets

Enhanced subnets configuration and management is now available from *Fabric View* with additional support for nested subnet groups and tags.

## To view enhanced subnets in FortiAnalyzer:

### 1. Go to *Fabric View > Fabric > Subnets*.

The subnets and subnet groups table is shown displaying additional information including the created time, update time, associated tags, and a description.

| Fabric View      |                            |                     |                     |            |             |  |
|------------------|----------------------------|---------------------|---------------------|------------|-------------|--|
| Fabric           |                            |                     |                     |            |             |  |
| Subnets          |                            |                     |                     |            |             |  |
| Subnet (5)       |                            |                     |                     |            |             |  |
| Name             | Details                    | Create Time         | Update Time         | Tags       | Description |  |
| Finance          | 10.100.92.100-10.100.92.10 | 2021-04-20 12:18:22 | 2021-04-20 12:18:22 | Finance    |             |  |
| Management       | 10.100.55.100-10.100.55.10 | 2021-04-20 12:18:27 | 2021-04-20 12:18:27 | Management |             |  |
| Marketing_02     | 192.168.50.1-192.168.50.99 | 2021-04-20 12:14:01 | 2021-04-20 12:18:41 | Marketing  |             |  |
| Sales            | 10.100.94.100-10.100.94.10 | 2021-04-20 12:18:17 | 2021-04-20 12:18:17 | Sales      |             |  |
| marketing        | 10.100.91.100-10.100.91.10 | 2021-04-20 12:18:32 | 2021-04-20 12:18:32 | Marketing  |             |  |
| Subnet Group (2) |                            |                     |                     |            |             |  |
| Group_01         | Finance                    | 2021-04-20 12:14:20 | 2021-04-20 12:14:20 |            |             |  |
| Group_02         | Finance                    | 2021-04-20 12:18:11 | 2021-04-20 12:18:11 | Group2     |             |  |

### 2. Edit or create a new subnet group.

Subnet groups have additional configurable options including a description field and tag support. Tags are shown in the *Asset Center* list if the endpoint IP falls within the subnet group.

Subnet groups support nested groups as members.

### 3. Edit or create a new subnet.

Subnets have additional configurable options including a description field and tag support. Tags are shown in the *Asset Center* list if the endpoint IP falls within the subnet.

4. Go to *Log View > FortiAnalyzer > Events*. Local events are generated when subnets are created, updated, or deleted.
5. Reports and Event Handlers can use subnets as filters.

## Incident and Event Management

This section lists the new features added to FortiAnalyzer for incident and event management:

- [FortiClient event handler update on page 32](#)
- [FortiDeceptor default handler on page 33](#)
- [IPS signatures on-hold event handler on page 34](#)
- [NOC event handlers on page 36](#)

## FortiClient event handler update

The predefined FortiClient event handlers are updated to include the detection from the newly added logs.

### To view the updated FortiClient event handlers:

#### 1. Go to *FortiSoC > Handlers > Event Handler List*.

Predefined handlers providing threat detection on FortiClient logs are available. These event handlers are disabled by default.

| FCT                                 |        |                                                     |                                                                                                                                                                                                                                                                                                     |             |               |              |
|-------------------------------------|--------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|--------------|
| <input type="checkbox"/>            | Status | Name                                                | Filters                                                                                                                                                                                                                                                                                             | Devices     | Send Alert to | Events       |
| <input type="checkbox"/>            |        | Default-FW-Compromised Host-Detection-IOC-By-Threat | > 3 Filters                                                                                                                                                                                                                                                                                         | All Devices |               |              |
| <input checked="" type="checkbox"/> |        | Default-FCT-Threat-Detection-By-Threat              | > 2 Filters<br>Filter 1 (Default,By_Threat,Malware)<br>clientfeature="av" and msg~"Found virus"<br>Filter 2 (Default,By_Threat,URL,Risky)<br>utmevent="webfilter" and utmaction="blocked"                                                                                                           | All Devices |               | 4            |
| <input checked="" type="checkbox"/> |        | Default-FCT-Threat-Detection-By-Endpoint            | > 3 Filters<br>Filter 1 (Default,By_Endpoint,Sandbox,Malware)<br>clientfeature="sandboxing" and msg~"Found virus"<br>Filter 2 (Default,By_Endpoint,Malware)<br>clientfeature="av" and msg~"Found virus"<br>Filter 3 (Default,By_Endpoint,URL,Risky)<br>utmevent="webfilter" and utmaction="blocked" | All Devices |               | 4            |
| <input type="checkbox"/>            |        | Default-Sandbox-Detections-By-Threat                | > 10 Filters                                                                                                                                                                                                                                                                                        | All Devices |               | > 69 Subnets |
| <input type="checkbox"/>            |        | Default-Risky-Destination-Detection-By-Threat       | > 15 Filters                                                                                                                                                                                                                                                                                        | All Devices |               | > 77 Subnets |
| <input type="checkbox"/>            |        | Default-Malicious-File-Detection-By-Threat          | > 8 Filters                                                                                                                                                                                                                                                                                         | All Devices |               | > 77 Subnets |

#### 2. Double-click a FortiClient event handler to view filter details.

Edit Handler: Default-FCT-Threat-Detection-By-Threat

Filters (2)

Filter 1 ☒

Log Device Type: FortiClient  
Log Type: Event Log (fct-event)  
Group By: Virus Name (virus)  
Source Endpoint (endpoint)

Logs match: ☒ All ☐ Any of the following conditions

| Log Field                                                     | Match Criteria | Value |
|---------------------------------------------------------------|----------------|-------|
| <div>Click to add</div>                                       |                |       |
| Generic Text Filter: clientfeature="av" and msg~"Found virus" |                |       |

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: Malware found by FCT AV scan on File System

Event Status: Contained

☐ Allow FortiAnalyzer to choose

Event Severity: High

Tags: Malware

Additional Info: ☐ Use system default

Factory Reset OK Cancel

3. In the event handler list, right-click a FortiClient event handler and select *Enable*. After being enabled, events will be generated by the event handler.

| All Devices   All   Expand All   Show Acknowledged   Refresh   Custom View   Download |                                             |              |                   |     |          |                                          |                     |               |
|---------------------------------------------------------------------------------------|---------------------------------------------|--------------|-------------------|-----|----------|------------------------------------------|---------------------|---------------|
| Handler = "Default-FCT-Threat-Detection-By"   Add Filter                              |                                             |              |                   |     |          |                                          |                     |               |
| #                                                                                     | Event                                       | Event Status | Event Type        | Col | Severity | Handler                                  | First Occurrence    | Last Update   |
| 1                                                                                     | Malware_fam.gw (1)                          |              |                   |     |          |                                          |                     |               |
|                                                                                       | Malware found by FCT AV scan on File System | Contained    | FortiClient Event | 2   | High     | Default-FCT-Threat-Detection-By Threat   | 2021-02-03 15:15:59 | 2021-02-03 15 |
| 2                                                                                     | VAN-200578-PC1 (4)                          |              |                   |     |          |                                          |                     |               |
|                                                                                       | Malware found by FCT AV scan on File System | Contained    | FortiClient Event | 2   | High     | Default-FCT-Threat-Detection-By Endpoint | 2021-02-03 15:15:59 | 2021-02-03 15 |
|                                                                                       | Malware found by FCT AV scan on File System | Contained    | FortiClient Event | 2   | High     | Default-FCT-Threat-Detection-By Endpoint | 2021-02-03 15:15:59 | 2021-02-03 15 |
|                                                                                       | Malware found by FCT scan on File System    | Contained    | FortiClient Event | 4   | High     | Default-FCT-Threat-Detection-By Endpoint | 2021-02-03 15:15:59 | 2021-02-03 15 |
|                                                                                       | Malware found by FCT AV scan on File System | Contained    | FortiClient Event | 22  | High     | Default-FCT-Threat-Detection-By Endpoint | 2021-02-03 15:15:59 | 2021-02-03 15 |
| 3                                                                                     | W32/Parite.B (1)                            |              |                   |     |          |                                          |                     |               |
|                                                                                       | Malware found by FCT AV scan on File System | Contained    | FortiClient Event | 2   | High     | Default-FCT-Threat-Detection-By Threat   | 2021-02-03 15:15:59 | 2021-02-03 15 |
| 4                                                                                     | Adware/TEST_FILE (1)                        |              |                   |     |          |                                          |                     |               |
|                                                                                       | Malware found by FCT AV scan on File System | Contained    | FortiClient Event | 4   | High     | Default-FCT-Threat-Detection-By Threat   | 2021-02-03 15:15:59 | 2021-02-03 15 |
| 5                                                                                     | EICAR_TEST_FILE (1)                         |              |                   |     |          |                                          |                     |               |
|                                                                                       |                                             | Contained    | FortiClient Event | 22  | High     | Default-FCT-Threat-Detection-By Threat   | 2 minutes ago       | 2 minutes ago |

## FortiDeceptor default handler

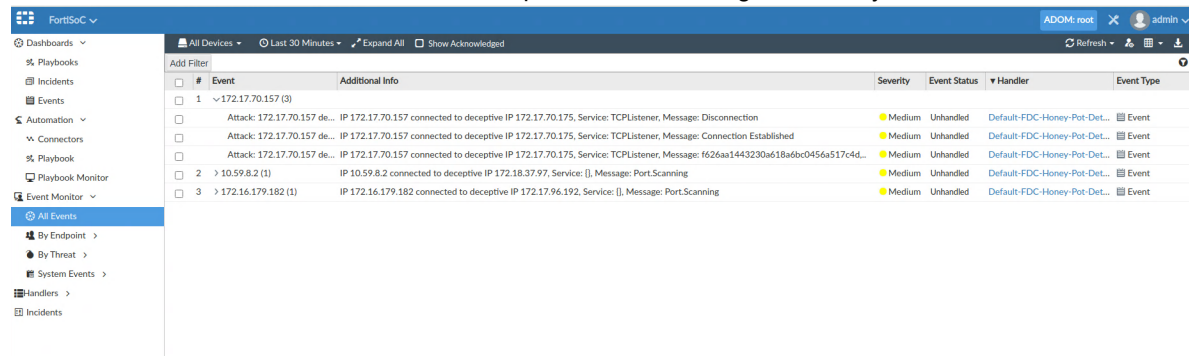
This is a new default handler that helps detect early breach activities and identify threats.

To use the FortiDeceptor default handler:

- Go to *FortiSoC > Handlers > Event Handler List*. In the event handler list, find *Default-FDC-Honey-Pot-Detection*.
- Right-click on the handler and select *Enable*.

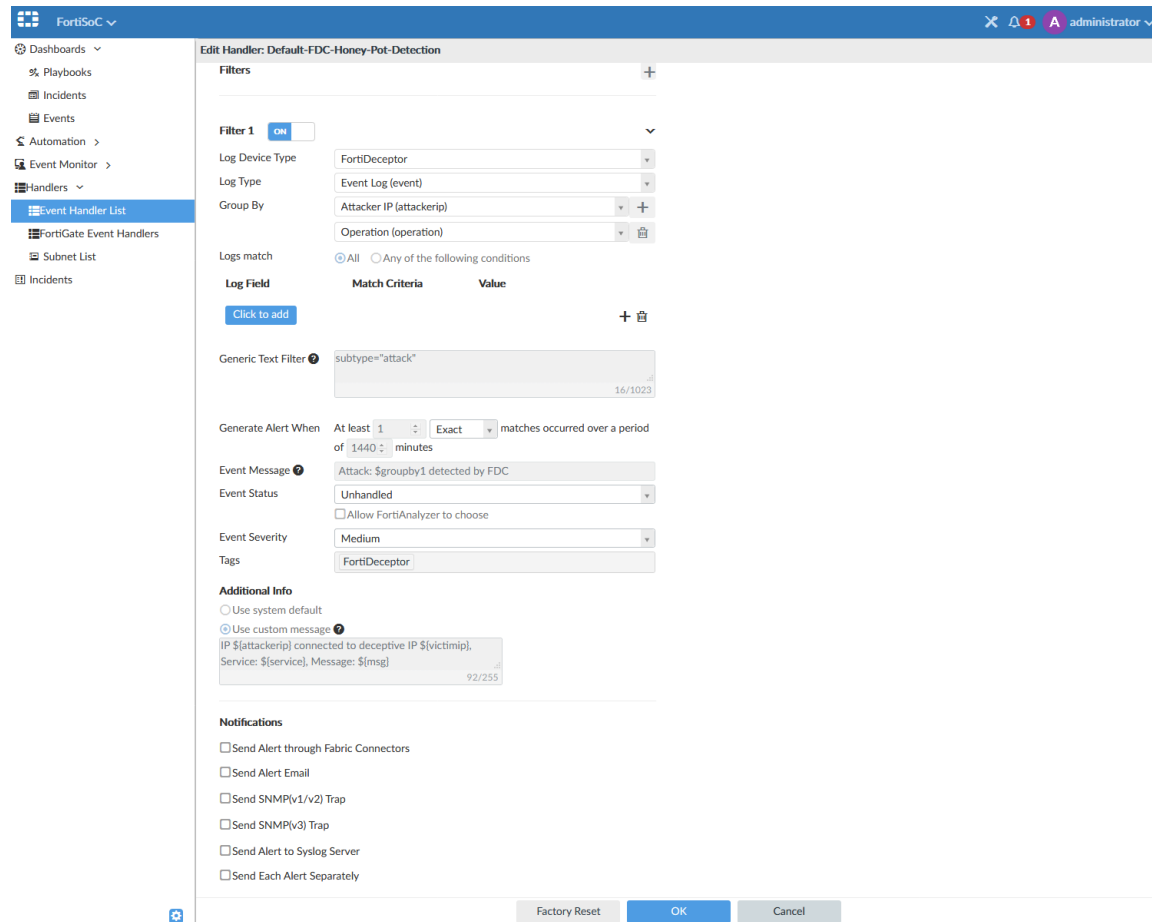
| FortiSoC   administrator                    |                                                  |              |              |               |        |                  |                  |  |
|---------------------------------------------|--------------------------------------------------|--------------|--------------|---------------|--------|------------------|------------------|--|
| + Create New   Edit   Delete   Clone   More |                                                  |              |              |               |        |                  |                  |  |
| Status                                      | Name                                             | Filters      | Devices      | Send Alert to | Events | Included Subnets | Excluded Subnets |  |
| <input type="checkbox"/>                    | Default-FortiSandbox-System-Handler              | > 3 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default-FortiSandbox-Malware-Handler             | > 2 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default-FML-Threat-Detection-By-Email            | > 11 Filters | All Devices  |               |        |                  |                  |  |
| <input checked="" type="checkbox"/>         | Default-FDC-Honey-Pot-Detection                  | > 1 Filter   | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_Routing_Events                       | > 5 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_Network_Events                       | > 3 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_Switch_Events                        | > 5 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_HA_Events                            | > 4 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_Wireless_Events                      | > 4 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_Security_Events                      | > 4 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_Fabric_Events                        | > 7 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_System_Events                        | > 5 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_VPN_Events                           | > 7 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default_NOC_SD-WAN_Events                        | > 9 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default-IPS_Signature_On_Hold                    | > 1 Filter   | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Local Device Event                               | > 1 Filter   | Local Device |               | 2      |                  |                  |  |
| <input type="checkbox"/>                    | Default_FOS_System_Events                        | > 8 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default-Botnet-Communication-Detection-By-Threat | > 9 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default-Data-Leak-Detection-By-Threat            | > 2 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default-Sandbox-Detections-By-Threat             | > 10 Filters | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default-Malicious-Code-Detection-By-Threat       | > 8 Filters  | All Devices  |               |        |                  |                  |  |
| <input type="checkbox"/>                    | Default-Risky-Destination-Detection-By-Threat    | > 9 Filters  | All Devices  |               |        |                  |                  |  |

The handler is now enabled. Below is an example of some events generated by the handler.



| # | Event                       | Additional Info                                                                                                              | Severity | Event Status | Handler                      | Event Type |
|---|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|----------|--------------|------------------------------|------------|
| 1 | 172.17.70.157 (3)           |                                                                                                                              |          |              |                              |            |
|   | Attack: 172.17.70.157 de... | IP 172.17.70.157 connected to deceptive IP 172.17.70.175, Service: TCPListener, Message: Disconnection                       | Medium   | Unhandled    | Default-FDC-Honey-Pot-Det... | Event      |
|   | Attack: 172.17.70.157 de... | IP 172.17.70.157 connected to deceptive IP 172.17.70.175, Service: TCPListener, Message: Connection Established              | Medium   | Unhandled    | Default-FDC-Honey-Pot-Det... | Event      |
|   | Attack: 172.17.70.157 de... | IP 172.17.70.157 connected to deceptive IP 172.17.70.175, Service: TCPListener, Message: f626aa1443230a618a6bc0456a517c4d... | Medium   | Unhandled    | Default-FDC-Honey-Pot-Det... | Event      |
| 2 | > 10.59.8.2 (1)             | IP 10.59.8.2 connected to deceptive IP 172.18.37.97, Service: [], Message: Port.Scanning                                     | Medium   | Unhandled    | Default-FDC-Honey-Pot-Det... | Event      |
| 3 | > 172.16.179.182 (1)        | IP 172.16.179.182 connected to deceptive IP 172.17.96.192, Service: [], Message: Port.Scanning                               | Medium   | Unhandled    | Default-FDC-Honey-Pot-Det... | Event      |

### 3. Double click on the handler in the list to review its filter details.



**Edit Handler: Default-FDC-Honey-Pot-Detection**

**Filters**

Filter 1 ☐ ON

Log Device Type: FortiDeceptor

Log Type: Event Log (event)

Group By: Attacker IP (attackerip)

Operation (operation)

Logs match: ☒ All ☐ Any of the following conditions

**Log Field**      **Match Criteria**      **Value**

[Click to add](#)      +

Generic Text Filter: subtype="attack" (16/1023)

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: Attack: \$groupby1 detected by FDC

Event Status: Unhandled

Event Severity: Medium

Tags: FortiDeceptor

**Additional Info**

☐ Use system default

☒ Use custom message

IP: \${attackerip} connected to deceptive IP \${victimip}, Service: \${service}, Message: \${msg} (92/255)

**Notifications**

☐ Send Alert through Fabric Connectors

☐ Send Alert Email

☐ Send SNMP(v1/v2) Trap

☐ Send SNMP(v3) Trap

☐ Send Alert to Syslog Server

☐ Send Each Alert Separately

Factory Reset      OK      Cancel

## IPS signatures on-hold event handler

A new event handler is available for admins to monitor FortiGate IPS logs for the IPS signatures that are on hold.

### To use the IPS signatures on-hold event handler:

- Go to *FortiSoC > Handlers > Event Handler List*.  
The *Default-IPS\_Signature\_On\_Hold* event handler is displayed and is disabled by default.

| + Create New Edit Delete Clone More |        |                                       |              |             |               |        |                  |                  |  |
|-------------------------------------|--------|---------------------------------------|--------------|-------------|---------------|--------|------------------|------------------|--|
| <input type="checkbox"/>            | Status | Name                                  | Filters      | Devices     | Send Alert to | Events | Included Subnets | Excluded Subnets |  |
| <input type="checkbox"/>            |        | Default-FCT-Threat-Detection-By-Thre  | > 2 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default-FCT-Threat-Detection-By-End   | > 3 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default-FSA-Malware-Handler-By-Thre   | > 6 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default-FSA-Malware-Handler-By-End    | > 4 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default-FSA-System-Handler            | > 3 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default-FML-Threat-Detection-By-Em    | > 11 Filters | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_Routing_Events            | > 5 Filters  | All Devices |               | 4      |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_Network_Events            | > 3 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_Switch_Events             | > 5 Filters  | All Devices |               | 249    |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_HA_Events                 | > 4 Filters  | All Devices |               | 3      |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_Wireless_Events           | > 4 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_Security_Events           | > 4 Filters  | All Devices |               | 2      |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_Fabric_Events             | > 7 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_System_Events             | > 5 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_VPN_Events                | > 7 Filters  | All Devices |               | 14     |                  |                  |  |
| <input type="checkbox"/>            |        | Default_NOC_SD-WAN_Events             | > 9 Filters  | All Devices |               |        |                  |                  |  |
| <input checked="" type="checkbox"/> |        | Default-IPS_Signature_On_Hold         | > 1 Filter   | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default FOS System Events             | > 8 Filters  | All Devices |               |        |                  |                  |  |
| <input type="checkbox"/>            |        | Default-Data-Leak-Detection-By-Threat | > 2 Filters  | All Devices |               |        |                  |                  |  |

Double-click the event handler to view its filter definition.

#### Edit Handler: Default-IPS\_Signature\_On\_Hold

Filters

+

Filter 1

ON

▼

Log Device Type

FortiGate

▼

Log Type

IPS (ips)

▼

Group By

Hostname (hostname)

▼

+

Attack Name (attack)

▼

🗑️

Logs match

☒ All ☐ Any of the following conditions

Log Field

Match Criteria

Value

Click to add

+

🗑️

Generic Text Filter ?

msg~"signature is on hold" and (logid==0419016384)

50/1023

Generate Alert When

At least 1

Exact

▼

matches occurred over a period of 1440

minutes

Event Message ?

Signature [ \$groupby2 ] is on hold

Event Status

(Blank)

▼

☐ Allow FortiAnalyzer to choose

Event Severity

High

▼

Tags

IPS

Signature

Hold

Additional Info

☐ Use system default

☒ Use custom message ?

\$(msg)

🗑️

Factory Reset

OK

Cancel

2. Right-click on the event handler in the event handlers list, and click *Enable*. Events will be generated for IPS signature that are on hold.

| All Devices All Expand All Show Acknowledged Refresh |                                                |                                                              |                    |                               |              |            |
|------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------|--------------------|-------------------------------|--------------|------------|
| Handler = "Default-IPS_Signature_On_Hold" Add Filter |                                                |                                                              |                    |                               |              |            |
| #                                                    | Event                                          | Additional Info                                              | Event ID           | Handler                       | Event Status | Event Type |
| 1                                                    | 172.16.200.55 (1)                              |                                                              |                    |                               |              |            |
|                                                      | Signature [ Eicar.Virus.Test.File ] is on hold | file_transfer: Eicar.Virus.Test.File, (signature is on hold) | 202102231000010448 | Default-IPS_Signature_On_Hold |              | IPS 1      |

## NOC event handlers

A new set of default event handlers are available for NOC to monitor network events and detect problems for routing, switching, wireless and more.

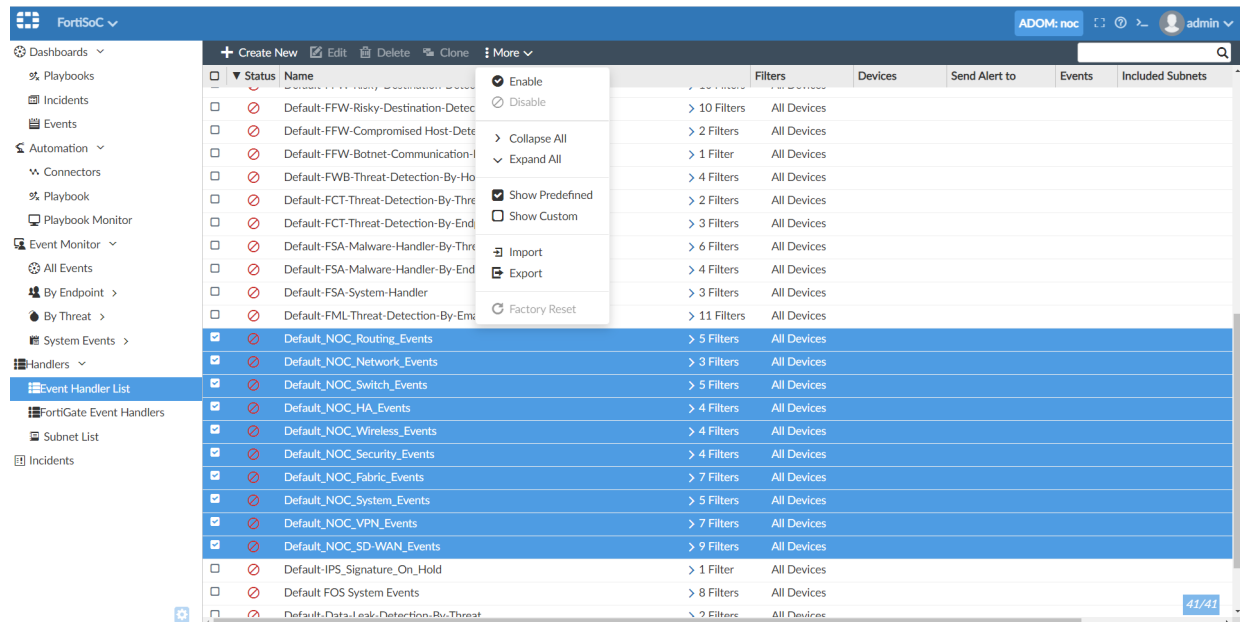
The following NOC event handlers are available in the *Event Handler List*:

- Default\_NOC\_Routing\_Events
- Default\_NOC\_Network\_Events
- Default\_NOC\_Switch\_Events
- Default\_NOC\_HA\_Events
- Default\_NOC\_Wireless\_Events
- Default\_NOC\_Security\_Events
- Default\_NOC\_Fabric\_Events
- Default\_NOC\_System\_Events
- Default\_NOC\_VPN\_Events
- Default\_NOC\_SD-WAN\_Events



## To enable NOC event handlers:

### 1. Go to *FortiSOC > Handlers > Event Handler List*.



## 2. Double-click a NOC event handler to view the predefined filters, and to enable notifications.

**Edit Handler: Default\_NOC\_Routing\_Events**

Filters (5)

**Filter 1** ☒

Log Device Type: FortiGate

Log Type: Event Log (event)

Log Subtype: Any (any...)

Group By: Device Name (devname)

Log Description (logdesc)

Logs match: ☐ All ☒ Any of the following conditions

| Log Field | Match Criteria | Value |
|-----------|----------------|-------|
|           |                |       |

[Click to add](#)

Generic Text Filter: logdesc="Routing information changed"

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: \$groupby1 \$groupby2

Event Status:

☒ Allow FortiAnalyzer to choose

Event Severity: Medium

Tags: NOC Routing

**Additional Info**

☐ Use system default

☒ Use custom message: \$(logdesc) on \$(devname) with message \$(msg)

**Filter 2** ☒

Log Device Type: FortiGate

Log Type: Event Log (event)

Log Subtype: Router (router)

Group By: Device Name (devname)

Log Description (logdesc)

Logs match: ☐ All ☒ Any of the following conditions

| Log Field | Match Criteria | Value |
|-----------|----------------|-------|
|           |                |       |

[Click to add](#)

Generic Text Filter: logdesc="BGP neighbor status changed"

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: \$groupby1 \$groupby2

Event Status:

☒ Allow FortiAnalyzer to choose

Event Severity: Medium

Tags: NOC Routing

**Additional Info**

☐ Use system default

☒ Use custom message: \$(devname), BGP neighbor status changed with message \$(msg)

**Filter 3** ☒

Log Device Type: FortiGate

Log Type: Event Log (event)

Log Subtype: Router (router)

Group By: Device Name (devname)

Log Description (logdesc)

Logs match: ☐ All ☒ Any of the following conditions

| Log Field | Match Criteria | Value |
|-----------|----------------|-------|
|           |                |       |

[Click to add](#)

Generic Text Filter: logdesc=="OSPF neighbor status changed" OR logdesc=="OSPF6 neighbor status changed"

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: \$groupby1 \$groupby2

Event Status:

☒ Allow FortiAnalyzer to choose

Event Severity: Medium

Tags: NOC Routing

**Additional Info**

☐ Use system default

☒ Use custom message: \$(logdesc) on \$(devname) with message \$(msg)

**Filter 4** ☒

Log Device Type: FortiGate

Log Type: Event Log (event)

Log Subtype: Router (router)

Group By: Device Name (devname)

Log Description (logdesc)

Logs match: ☐ All ☒ Any of the following conditions

| Log Field | Match Criteria | Value |
|-----------|----------------|-------|
|           |                |       |

[Click to add](#)

Generic Text Filter: logdesc=="neighbor table change"

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: \$groupby1 \$groupby2

Event Status:

☒ Allow FortiAnalyzer to choose

Event Severity: Medium

Tags: NOC Routing

**Additional Info**

☐ Use system default

☒ Use custom message: \$(logdesc) on \$(devname) with message \$(msg)

**Filter 5** ☒

Log Device Type: FortiGate

Log Type: Event Log (event)

Log Subtype: Router (router)

Group By: Device Name (devname)

Log Description (logdesc)

Logs match: ☐ All ☒ Any of the following conditions

| Log Field | Match Criteria | Value |
|-----------|----------------|-------|
|           |                |       |

[Click to add](#)

Generic Text Filter: logdesc=="VRRP state changed"

Generate Alert When: At least 1 Exact matches occurred over a period of 1440 minutes

Event Message: \$groupby1 \$groupby2

Event Status:

☒ Allow FortiAnalyzer to choose

Event Severity: Medium

Tags: NOC Routing

**Additional Info**

☐ Use system default

☒ Use custom message: \$(logdesc) on \$(devname) with message \$(msg)

### 3. In the toolbar click *More > Enable*. The handler will generate events from a NOC perspective.

| # | Event                                                                  | Event Stat | Event Type | Col    | Severity    | Handler       | Additional Info                                              | First Occurrence    | Last Update     |
|---|------------------------------------------------------------------------|------------|------------|--------|-------------|---------------|--------------------------------------------------------------|---------------------|-----------------|
| 1 | > FGT_SVN_JENKINS (362)                                                | ...        | ...        | 8...   | Critical    | ...           | ...                                                          | 7 days ago          | In a few sec... |
| 2 | > Van_DC_Srv221 (38)                                                   | ...        | ...        | 1...   | High        | ...           | ...                                                          | 7 days ago          | In a few sec... |
| 3 | > Van_Office_FW2 (439)                                                 | ...        | ...        | ...    | ...         | ...           | ...                                                          | ...                 | ...             |
|   | Van_Office_FW2 primary switch port31 has come up                       | Others     | 97         | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 16:40:10 | 2021-02-10      |
|   | Van_Office_FW2 IPsec phase 1 error detected                            | VPN        | 9...       | High   | Default_NOC | VPN_Events    | IPsec phase 1 error due to: negotiate_error with reason: ... | 2021-02-10 16:00:00 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port31 has gone down                     | Others     | 96         | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 16:40:22 | 2021-02-10      |
|   | Van_Office_FW2 FortiSwitch system vlan interface change has occurred   | Others     | 52         | Medium | Default_NOC | switch_Events | Device Van_Office_FW2 interface vlan change with mess...     | 2021-02-10 16:00:11 | 2021-02-10      |
|   | Van_Office_FW2 Disconnected from FortiAnalyzer 172.18.3.226            | System     | 2...       | High   | Default_NOC | fabric_Events | Disconnected from FortiAnalyzer 172.18.3.226                 | 2021-02-10 16:00:11 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port26 has come up                       | Others     | 2...       | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 16:00:14 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port26 has gone down                     | Others     | 2...       | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 16:00:12 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port4 has come up                   | Others     | 3          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 16:00:28 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port4 has gone down                 | Others     | 3          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 16:00:23 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port7 has come up                   | Others     | 4          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 18:02:13 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port7 has gone down                 | Others     | 4          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 18:02:09 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port16 has come up                  | Others     | 3          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 17:58:17 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port16 has gone down                | Others     | 3          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 17:58:14 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port38 has come up                  | Others     | 2          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 17:48:36 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port38 has gone down                | Others     | 2          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 17:48:33 | 2021-02-10      |
|   | Van_Office_FW2 IPsec phase 2 status change                             | VPN        | 8          | Medium | Default_NOC | VPN_Events    | IPsec phase 2 status changed due to: phase2-down...          | 2021-02-10 16:13:57 | 2021-02-10      |
|   | Van_Office_FW2 security fabric settings change: Connection with CSF... | System     | 1          | Medium | Default_NOC | fabric_Events | Device: Van_Office_FW2 change with message: Connect...       | 2021-02-10 17:17:48 | 2021-02-10      |
|   | Van_Office_FW2 security fabric settings change: Connection with aut... | System     | 1          | Medium | Default_NOC | fabric_Events | Device: Van_Office_FW2 change with message: Disconn...       | 2021-02-10 17:17:36 | 2021-02-10      |
|   | Van_Office_FW2 Disconnected from Cooperative Security Fabric me...     | System     | 1          | High   | Default_NOC | fabric_Events | Connection with authorized CSF member terminated on...       | 2021-02-10 17:17:36 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port1 has gone down                 | Others     | 1          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 17:15:20 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port25 has come up                  | Others     | 3          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 17:13:57 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port25 has gone down                | Others     | 3          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 17:13:55 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port41 has gone down                | Others     | 1          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 17:02:33 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port48 has come up                  | Others     | 7          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 16:43:13 | 2021-02-10      |
|   | Van_Office_FW2 primary switch port port48 has gone down                | Others     | 7          | Medium | Default_NOC | switch_Events | FortiSwitch link on Device: Van_Office_FW2 with messa...     | 2021-02-10 16:43:10 | 2021-02-10      |

## Dashboards

This section lists the new features added to FortiAnalyzer for dashboards:

- [Shadow IT Monitoring Service on page 39](#)
- [Data sources tuning on page 42](#)
- [Asset and Identity Dashboards on page 46](#)

## Shadow IT Monitoring Service

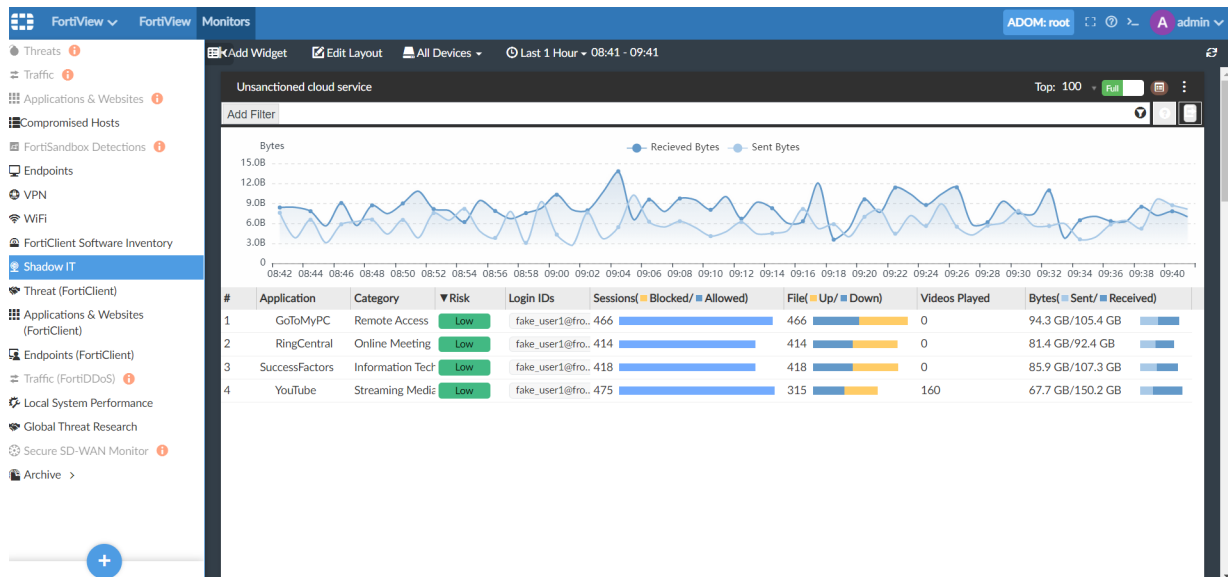
The Shadow IT dashboard continuously monitors customer environments by correlating data from FortiOS and FortiCASB to discover and investigate the risk of shadow IT and remediate and control the security risks.

To use this feature, you must have a FortiCASB account subscribed for SaaS features, and a FortiCASB connector configured on FortiAnalyzer.

### To view the Shadow IT dashboard:

1. Go to *FortiView > Monitors* and select *Shadow IT* from the tree menu.  
The Shadow IT dashboard has the following widgets:

## a. Unsanctioned Cloud Service.



## b. Non-federated Users with File Access.

The screenshot displays the FortiView Monitors interface for 'Non-federated users with file access'. The left sidebar shows various security categories, with 'Shadow IT' selected. The main panel features a table listing applications, users, and the number of files accessed.

| #  | Application | User                                                    | # of Files |
|----|-------------|---------------------------------------------------------|------------|
| 1  | Salesforce  | jiangli.jessica@gmail.com                               | 0          |
| 2  | Salesforce  | zhangyue_1981@hotmail.com                               | 0          |
| 3  | Office365   | jessica_ext@forticasbdev.onmicrosoft.com                | 0          |
| 4  | Salesforce  | yyao2@fortinet.com                                      | 2          |
| 5  | Office365   | guest_fortinet@forticasbdev.onmicrosoft.com             | 0          |
| 6  | Office365   | jessica_yahoo@forticasbdev.onmicrosoft.com              | 0          |
| 7  | Office365   | yuezhang_fortinet.com#EXT#@binxufortinet.onmicrosoft.c  | 0          |
| 8  | Office365   | acappadonia.azure_gmail.com#EXT#@binxufortinet.onmicr   | 0          |
| 9  | Office365   | lijiang_fortinet.comXXXXXX@forticasbdev.onmicrosoft.com | 0          |
| 10 | Office365   | mh20110503_gmail.com#EXT#@casbqa1.onmicrosoft.com       | 0          |
| 11 | Office365   | testadmin1_forticasb.com#EXT#@binxufortinet.onmicrosof  | 0          |
| 12 | Office365   | zabaneh34_hotmail.com#EXT#@binxufortinet.onmicrosoft.   | 0          |
| 13 | Salesforce  | mh20110503@guest.fortinet.com                           | 0          |

## c. File Exfiltration Detection.

| #  | From Application | To Application           | User                | IP              | File Name                      | Data Pattern |
|----|------------------|--------------------------|---------------------|-----------------|--------------------------------|--------------|
| 1  | Dropbox          | YouTube_Video.Play       | fake_user2@from.log | 71.168.79.118   | 22-ca-passport_publiclink.pptx |              |
| 2  | Dropbox          | YouTube_Video.Play       | fake_user6@from.log | 159.54.91.3     | 22-ca-passport_publiclink.pptx |              |
| 3  | Dropbox          | YouTube_Video.Play       | fake_user9@from.log | 224.72.216.155  | 22-ca-passport_publiclink.pptx |              |
| 4  | Dropbox          | GoToMyPC_File.Download   | fake_user4@from.log | 62.168.35.188   | 22-ca-passport_publiclink.pptx |              |
| 5  | Dropbox          | GoToMyPC_File.Download   | fake_user1@from.log | 192.224.33.213  | 22-ca-passport_publiclink.pptx |              |
| 6  | Dropbox          | Salesforce_File.Download | fake_user3@from.log | 151.107.119.170 | 22-ca-passport_publiclink.pptx |              |
| 7  | Dropbox          | Office365_File.Download  | fake_user1@from.log | 104.215.172.113 | 22-ca-passport_publiclink.pptx |              |
| 8  | Dropbox          | Salesforce_File.Download | fake_user3@from.log | 252.26.42.184   | 22-ca-passport_publiclink.pptx |              |
| 9  | Dropbox          | statics.dropbox.com      | fake_user3@from.log | 57.93.147.214   | 22-ca-passport_publiclink.pptx |              |
| 10 | Dropbox          | banana_File.Download     | fake_user6@from.log | 205.59.113.20   | 22-ca-passport_publiclink.pptx |              |
| 11 | Dropbox          | Facebook_File.Download   | fake_user3@from.log | 104.148.14.52   | 22-ca-passport_publiclink.pptx |              |
| 12 | Dropbox          | banana_File.Download     | fake_user8@from.log | 246.128.228.84  | 22-ca-passport_publiclink.pptx |              |
| 13 | Dropbox          | banana_File.Download     | fake_user6@from.log | 175.161.67.252  | 22-ca-passport_publiclink.pptx |              |
| 14 | Dropbox          | YouTube_Video.Play       | fake_user7@from.log | 134.95.79.2     | 22-ca-passport_publiclink.pptx |              |
| 15 | Dropbox          | GoToMyPC_File.Download   | fake_user7@from.log | 193.140.58.26   | 22-ca-passport_publiclink.pptx |              |
| 16 | Dropbox          | Facebook_File.Download   | fake_user6@from.log | 95.88.115.218   | 22-ca-passport_publiclink.pptx |              |
| 17 | Dropbox          | Office365_File.Download  | fake_user8@from.log | 216.57.61.178   | 22-ca-passport_publiclink.pptx |              |
| 18 | Dropbox          | statics.dropbox.com      | fake_user7@from.log | 60.245.174.125  | 22-ca-passport_publiclink.pptx |              |

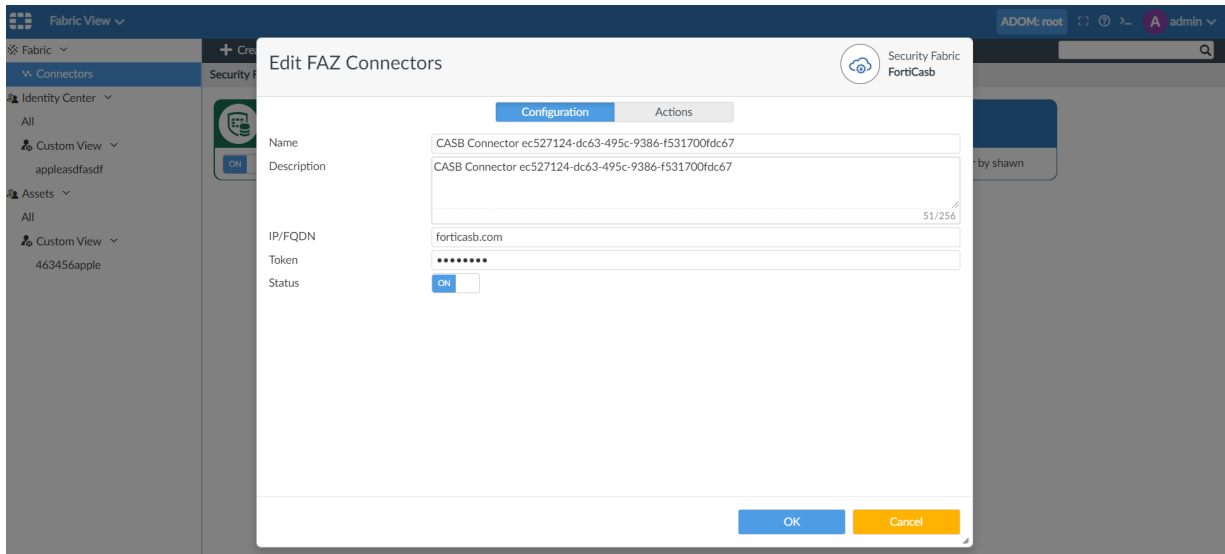
## d. Non-federated Users with Cloud Access.

| #  | Application | User                                                           | Permissions                                                      |
|----|-------------|----------------------------------------------------------------|------------------------------------------------------------------|
| 1  | Salesforce  | jiangli.jessica@gmail.com                                      | Chatter External                                                 |
| 2  | Salesforce  | zhangyue_1981@hotmail.com                                      | Chatter External                                                 |
| 3  | Office365   | jessica_ext@forticasbdev.onmicrosoft.com                       | Security Administrator                                           |
| 4  | Salesforce  | yyao2@fortinet.com                                             | Chatter External                                                 |
| 5  | Office365   | guest_fortinet@forticasbdev.onmicrosoft.com                    | Intune Service Administrator Security Administrator Compliance A |
| 6  | Office365   | jessica_yahoo@forticasbdev.onmicrosoft.com                     |                                                                  |
| 7  | Office365   | yuezhang_fortinet.com#EXT#@binxufortinet.onmicrosoft.com       |                                                                  |
| 8  | Office365   | acappadonia.azure_gmail.com#EXT#@binxufortinet.onmicrosoft.com |                                                                  |
| 9  | Office365   | lijiang_fortinet.comXXXXXX@forticasbdev.onmicrosoft.com        | Global Administrator Directory Writers                           |
| 10 | Office365   | mh20110503_gmail.com#EXT#@casbqa1.onmicrosoft.com              |                                                                  |
| 11 | Office365   | testadmin1_forticasb.com#EXT#@binxufortinet.onmicrosoft.com    |                                                                  |
| 12 | Office365   | zabaneh34_hotmail.com#EXT#@binxufortinet.onmicrosoft.com       |                                                                  |
| 13 | Salesforce  | mh20110503@guest.fortinet.com                                  | Chatter External                                                 |

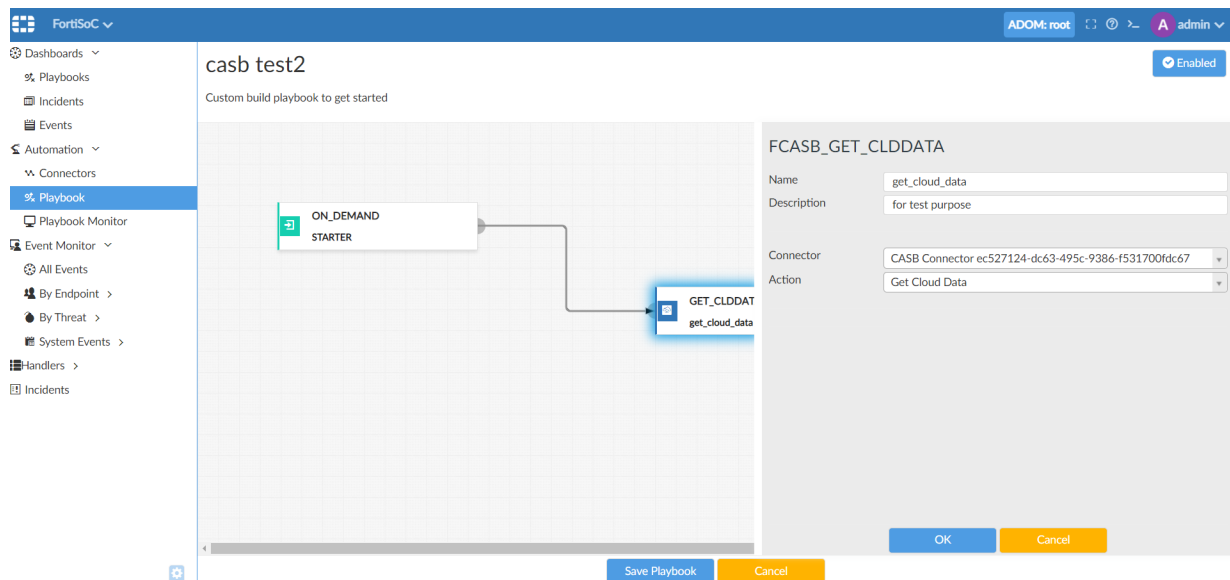
2. In order for FortiAnalyzer to correlate data from FortiGate and FortiCASB to generate the log data used in the Shadow IT monitor, an administrator must configure the FortiCASB connector in FortiAnalyzer's *Fabric View*. When creating or editing a FortiCASB connector, enter the following information:

- **Name:** Enter a name for the FortiCASB connector.
- **Description:** (Optional) Enter a description of the connector.
- **IP/FQDN:** Enter the FortiCASB FQDN for your chosen server location. The server location is selected when creating your FortiCASB account. Use `forticasb.com` for global servers or `eu.forticasb.com` for EU based servers.
- **Token:** Enter the credentials token used for authentication. To create a FortiCASB credentials token, log in to FortiCASB with your account, go to *Home > Manage Company > API Setting*, and click *Generate New*. For more information, see *FortiCASB* on the [Fortinet Docs Library](#).

- **Status:** Set the status to *ON*.



- To retrieve cloud application, users, and sensitive file information from FortiCASB on demand, an administrator can configure a playbook on FortiAnalyzer in FortiSOC. The playbook must include a task configured with the FortiCASB connector and *Get Cloud Data* action.



## Data sources tuning

FortiAnalyzer 7.0.0 includes the option to have more granular control on data sources from the Asset Center and Identity Center - subnets can now be excluded from the selected data sources to reduce noise.

## To configure data sources:

1. Go to *Fabric View > Identity Center > All* or *Fabric View > Asset Center > All*.
2. Click the tools icon in the top-right corner of the pane, and select *Data Sources*.

The top screenshot shows the Identity Center view with the following table:

| Endpoint Name   | Tags | User | MAC Address       | IP Address   | FortiClient UUID | Hardware / OS Software | Vulnerabilities | Last Update         |
|-----------------|------|------|-------------------|--------------|------------------|------------------------|-----------------|---------------------|
| LAN-SALE-SIMULA |      |      | 00:06:5b:92:8e:f9 | 10.100.94.19 |                  | Linux                  |                 | 2021-04-21 16:09:24 |
| 10.100.88.15    |      |      | 02:09:0f:00:04:08 | 10.100.88.15 |                  |                        |                 | 2021-04-21 16:08:59 |
| LAN-FINANCE     |      |      | f4:03:04:cb:c6:b0 | 10.100.92.14 |                  | Linux                  |                 | 2021-04-21 16:09:26 |
| Y-BRANCH-01-CUS |      |      | 00:06:5b:d7:47:11 | 10.1.0.13    |                  | Linux                  |                 | 2021-04-23 11:17:05 |
| 10.100.88.14    |      |      | 02:09:0f:00:04:03 | 10.100.88.14 |                  |                        |                 | 2021-04-21 16:08:59 |
| LAN-PSW-GUEST   |      |      | 00:03:93:bf:1e:aa | 10.200.1.11  |                  | Linux                  |                 | 2021-04-21 16:09:27 |

The bottom screenshot shows the Asset Center view with the following table:

| User Name    | User Group | Endpoints           | VPN IP | Identification Time | Last Seen           | Last Update         |
|--------------|------------|---------------------|--------|---------------------|---------------------|---------------------|
| Aaren Moss   |            | Aaren Moss Laptop   |        | 2021-04-21 16:08:54 | 2021-04-23 13:38:54 | 2021-04-21 16:08:54 |
|              |            | VAN-200213          |        |                     |                     |                     |
| Charlie Key  |            | Charlie Key Laptop  |        | 2021-04-21 16:08:54 | 2021-04-23 13:38:54 | 2021-04-21 16:08:54 |
| Shay Bailey  |            | Shay Bailey PC      |        | 2021-04-21 16:08:54 | 2021-04-23 13:38:54 | 2021-04-21 16:08:54 |
| Gabby Acosta |            | Gabby Acosta Laptop |        | 2021-04-21 16:08:54 | 2021-04-23 13:38:54 | 2021-04-21 16:08:54 |
|              |            | VAN-200233-PC       |        |                     |                     |                     |

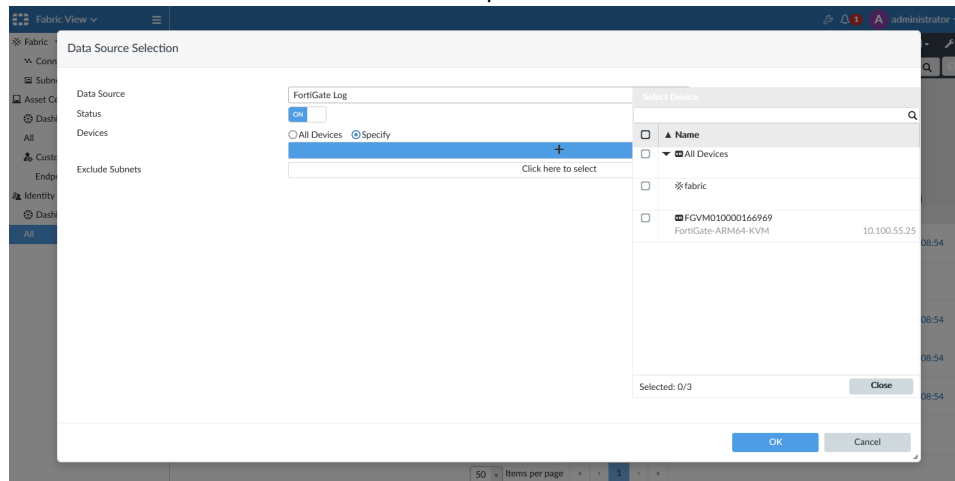
The *Data Source Selection* dialog appears.

The Data Source Selection dialog box shows the following table:

| # | Device Name/EMS | Device Type | Include | Exclude | Status  |
|---|-----------------|-------------|---------|---------|---------|
| 1 | All_FortiClient | FortiClient |         |         | Enabled |
| 2 | All_FortiGate   | FortiGate   |         |         | Enabled |

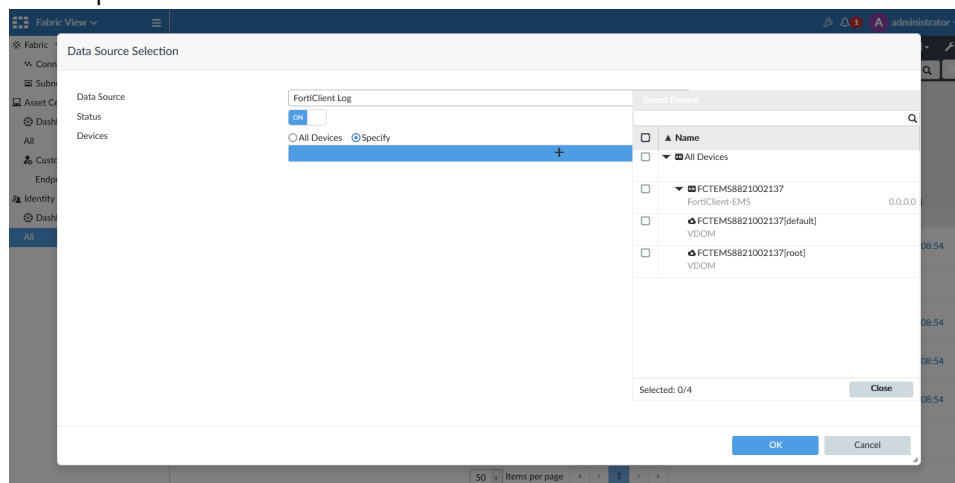
3. Click *Create New* to configure a new data source. Six data source types are available:
  - **FortiGate Log:**  
By default, the log identification of endpoints and end users is enabled for all devices and subnets. You can

create rules to specify which devices and which subnets can be excluded in the data source. Set the status to *OFF* to disable UEBA identification on the specified devices or all devices.



- **FortiClient Log:**

By default, the log identification of endpoints and end users is enabled for all devices. You can create rules to specify which devices can be excluded in the data source. Set the status to *OFF* to disable UEBA identification on the specified devices or all devices.

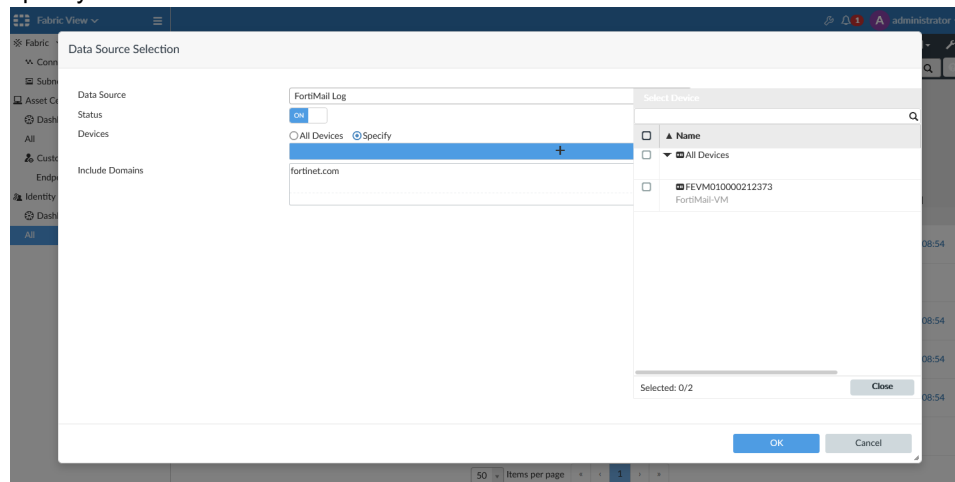


- **FortiMail Log:**

By default, the log identification of endpoints and end users is disabled for all devices. You can create rules to

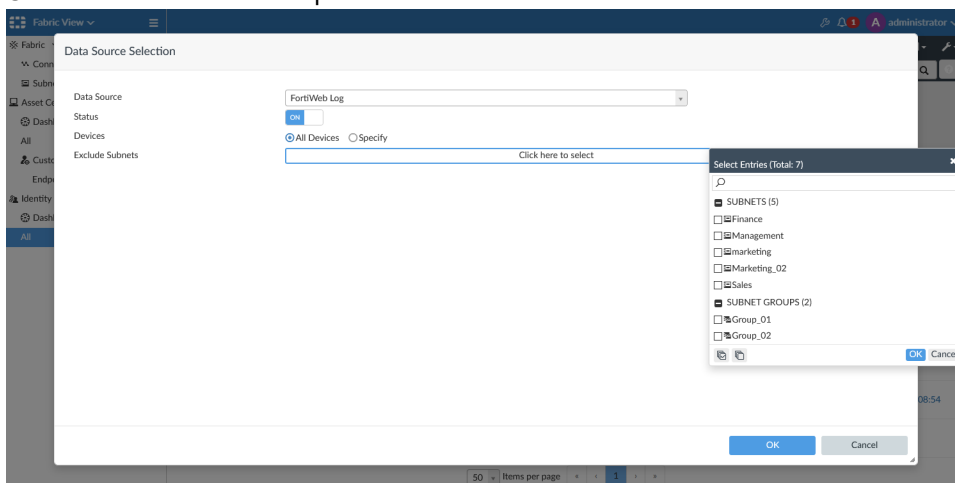


specify which devices and domains can be included in the data source.



- **FortiWeb Log:**

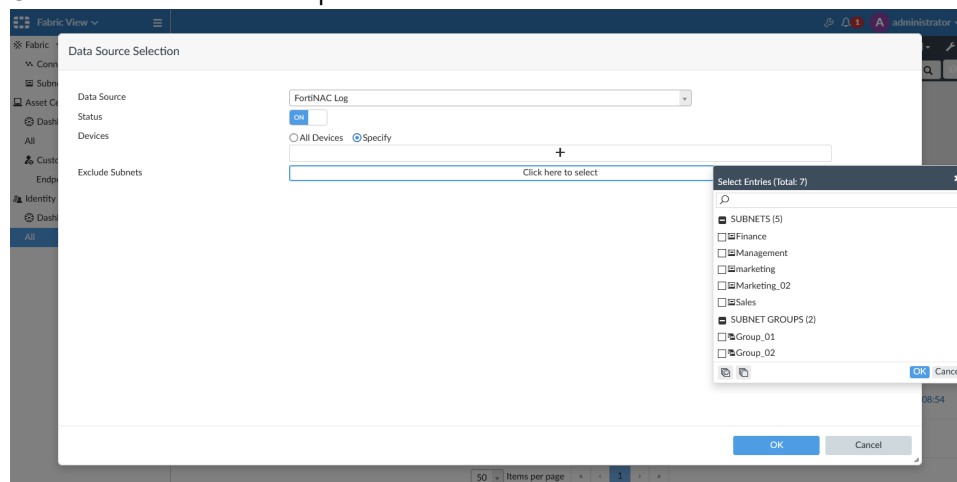
By default, the log identification of endpoints and end users is enabled for all devices. You can create rules to specify which devices and which subnets can be excluded in the data source. Set the status to *OFF* to disable UEBA identification on the specified devices or all devices.



- **FortiNAC Log:**

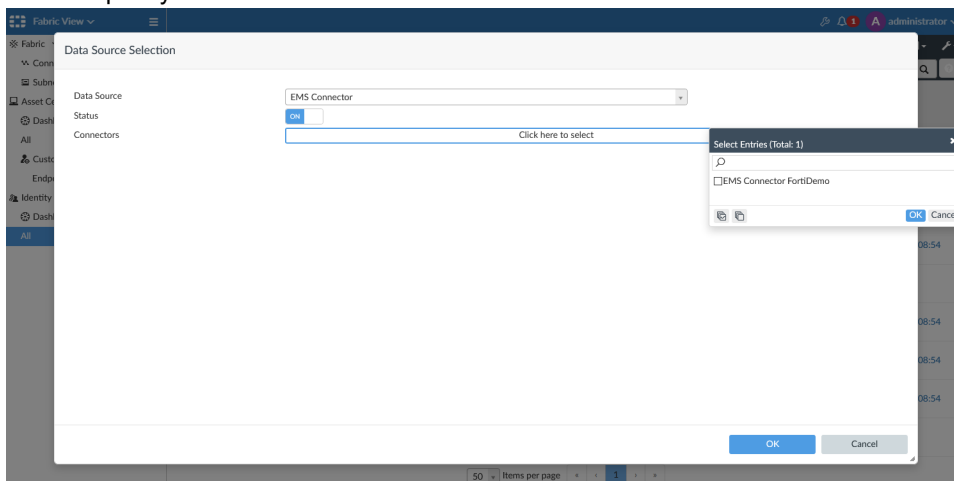
By default, the log identification of endpoints and end users is enabled for all devices. You can create rules to specify which devices and which subnets can be excluded in the data source. Set the status to *OFF* to disable

UEBA identification on the specified devices or all devices.



- **EMS Connector:**

By default, the log identification of endpoints and end users is disabled for all EMS connectors. You can create rules to specify which connectors can be included in the data source.



Rules on individual devices have higher priority than the rules configured for "All Devices". You can configure the same data source multiple times when the device or connector is unique. When a conflict arises, you will see a message indicating the data source for that device already exists, and you will have the option to override the existing data source.

## Asset and Identity Dashboards

Dedicated Assets/Identity dashboards to provide the SOC team better visibility on assets and their users.

### To view asset and identity dashboards:

1. Go to *Fabric View > Asset Center > Dashboard*.  
The Asset Center dashboard is displayed including twelve widgets.



Click on the donut or bar charts to view drilldown results.

Fabric View

Asset Center

Dashboard

All

Custom View (10)

Shawn

endpoint multiple user

Ottawa IT

Burnaby VPN Users

Burnaby Assets

High Severity Assets

Ottawa Assets

Ottawa TAC

ALI's PC

Burnaby Servers

Toggle Widgets

Detection Method

HW OS Distribution

Tag Distribution

Data Source Breakdown

18353

by\_fctuid

by\_mac

by\_ip

18353

AOS/00

APC Smart-UPS 3k

Android

Axis Firmware

Brother MFC-7820

Chrome OS

Cisco 2950, 2960,

Cisco Catalyst 260

DSM

Tag Distribution

Low

all\_registered\_clients

Burnaby

Workstation

FCT\_Enforce\_Linux\_Mac

0

1,000

2,000

3,000

4,000

Data Source Breakdown

FW\_Srv100

Corp\_EMS

VAN\_VPN\_Core1

Van\_Office\_FWI\_Master

Van\_Office\_FWI2

0

1,000

2,000

3,000

4,000

5,000

6,000

Last 1 Week • Mar 25 2021 - Apr 01 2021

Hardware / OS = "WIN64"

Add Filter

Endpoint Name

Tags

User

MAC Address

IP Address

FortiClient UUID

Source

Hardware

Software

Vulnerabilities

Identification method

Identification time

Last Seen

Last Update

1033

VAN-911878-LTO

Work

jean aabul

e4:5e:37:d1:2e:82

192.168.1.100

224C6335404C4BD4

Corp\_EMS/ WIN64

Details

2

23

by\_fctuid

2021-01-27 16:24:26

2021-03-29 10:40:29

2021-02-22 12:34:03

1041

VAN-200074-17

Low

jean aabul

98:90:96:a2:9d:c8

172.17.81.188

9E2DB44AA5D4B3

Corp\_EMS/ WIN64

Details

by\_fctuid

2021-01-27 16:24:26

2021-04-01 11:03:40

1074

VAN-909924-PC0

Low

jean aabul

e4:54:e8:c0:b1:d7

172.19.18.24

AEB4A377FF7E40E3

Corp\_EMS/ WIN64

Details

by\_fctuid

2021-01-27 16:24:26

2021-04-01 11:25:53

1084

VAN-906625-LTO

Low

jean aabul

ec:5c:68:77:a1:ab

10.0.0.195

8A92F9FD703B4CC

Corp\_EMS/ WIN64

Details

by\_fctuid

2021-01-27 16:24:26

2021-03-26 10:06:11

1086

WIN10-Jining

Low

jean aabul

f8:bc:12:9f:0b:86

192.168.1.80

FC0FAE87927A487B

Corp\_EMS/ WIN64

Details

by\_fctuid

2021-01-27 16:24:26

2021-04-01 07:07:40

1107

harpy-windows

Low

jean aabul

a4:c3:f0:62:accd

192.168.0.127

20D24540000D49D

Corp\_EMS/ WIN64

Details

16

23

by\_fctuid

2021-01-27 16:24:26

2021-04-01 11:19:45

50

Items per page

1

2

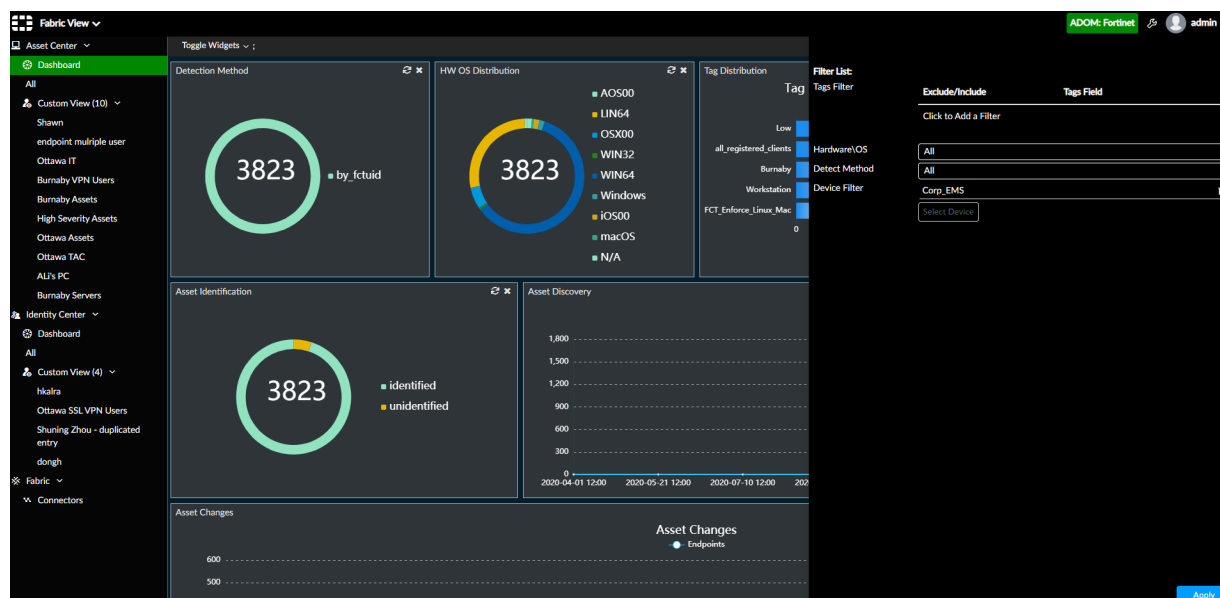
3

4

5

6

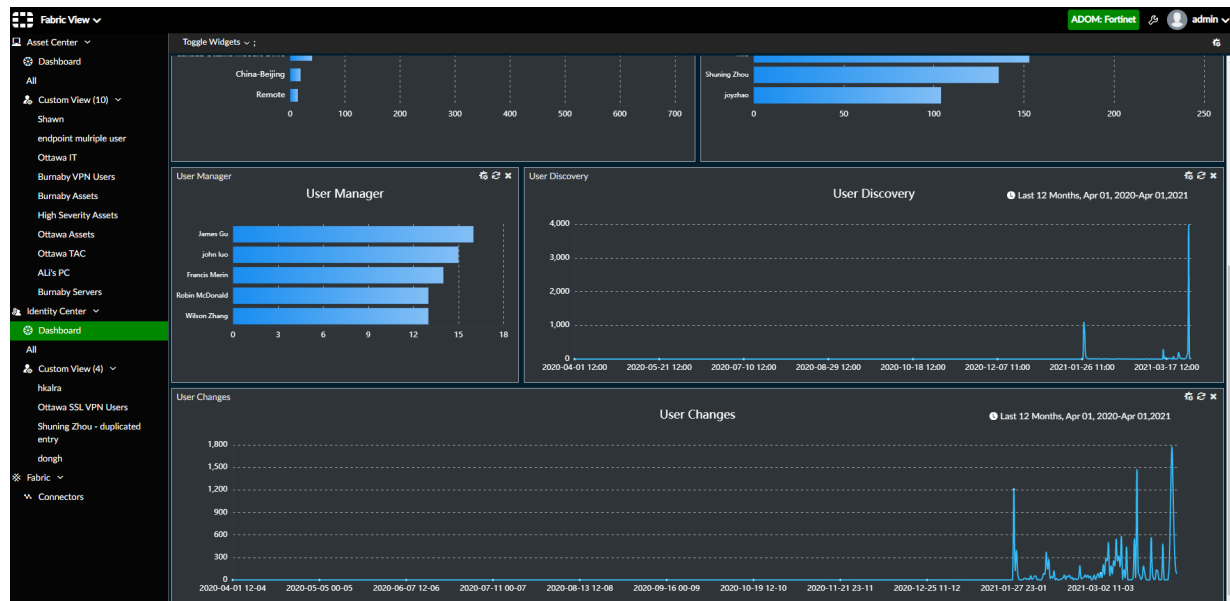
Click on the top-right filter icon to configure filters. For example, configure the filter to show endpoints from the device Corp\_EMS.



## 2. Go to *Fabric View > Identity Center > Dashboard*.

The Identity Center dashboard is displayed including seven widgets about end users.





# Log and Report

This section lists the new features added to FortiAnalyzer for logs and reports:

- [Logging on page 50](#)
- [Reports on page 65](#)

## Logging

This section lists the new features added to FortiAnalyzer for logging:

- [Improve log forwarding bandwidth efficiency on page 50](#)
- [Mask user data in log forwarder on page 55](#)
- [FortiEDR Central Manager logging on page 58](#)
- [FortiAI logging on FortiAnalyzer 7.0.1 on page 60](#)
- [Log forwarding enhancement 7.0.1 on page 64](#)

### Improve log forwarding bandwidth efficiency

FortiAnalyzer supports a new option to allow log data to be compressed for bandwidth optimization when forwarding the logs to a remote server in FortiAnalyzer format.

Log messages will be compressed when this feature is enabled and both FortiAnalyzer devices support the log compression feature. When log forwarding is configured with compression enabled to a remote FortiAnalyzer that does not support compression, the logs will remain uncompressed.

**To enable compression in log forwarding:**

1. Go to *System Settings > Log Forwarding*, and click *Create New*.
2. Select *FortiAnalyzer* as the *Remote Server Type*, and configure the server settings for your remote FortiAnalyzer.

- Set the *Compression* setting toggle to the *ON* position. It is set to *OFF* by default.

The screenshot shows the 'Edit Log Forwarding' configuration window in FortiAnalyzer. The left sidebar contains a menu with options like Dashboard, Logging Topology, All ADOMs, Storage Info, Network, HA, Admin, and Log Forwarding (which is selected). The main area is titled 'Edit Log Forwarding' and contains the following settings:

- Name: Demo
- Status: ☒ ON
- Remote Server Type: ☒ FortiAnalyzer, ☐ Syslog, ☐ Common Event Format(CEF)
- Server Address: 10.2.125.244
- Compression: ☒ ON
- Reliable Connection: ☒ ON
- Sending Frequency: ☒ Real-time, ☐ Every 1 Minute, ☐ Every 5 Minutes
- Log Forwarding Filters:
  - Device Filters: All FortiClient, FG100D3G00002900
  - Log Filters: ☐ OFF

At the bottom right, there are 'OK' and 'Cancel' buttons.

- Click **OK** to save the log forwarding configuration.

## Configuring log compression in the CLI

The following CLI setting has been added for log compression:

```
# set fwd-compression {enable|disable}
```

Following is an example of log forward configuration in the CLI:

```
config system log-forward
  edit 3
    set mode forwarding
    set fwd-max-delay realtime
    set server-name "demo"
    set server-addr "10.2.125.244"
    set fwd-reliable enable
    set fwd-compression enable
    set sync-metadata sf-topology interface-role device endusr-avatar
    set signature 6723252594909515930
  next
end
```

## Diagnosing log forward compression

The log format is displayed in `diagnose test application logfwd 3` and the compression ratio is displayed with `diagnose test application logfwd 4`.

**To view the log format:**

- In the FortiAnalyzer CLI, enter the following command:

```
diagnose test application logfwd 3
```

The output will include information about the log format.

```
#2: 244 => FortiAnalyzer @ 10.2.125.244:514 token=715983816682025708 Reliable Running
Updt=1610129597
tlvm-ver=2 logfwd-ver=1 logfmt=SiedLog compress
Grp=ld-244 Qid=21 Updt=1610129598 Hash=1.115f51236d8e2a20.0.0
- Dev-filter: FG100D3G00002901,FG100D3G00002900
```

### To view the compression ratio:

1. In the FortiAnalyzer CLI, enter the following command:

```
diagnose test application logfwd 4
```

The output will include information about the compression ratio.

```
** Server#1: 244 ld-244 Qid=21 Connected bind: from 16m42s ago
nmsg-sent=9978 nlog-sent=452083 send_timeout=0 send_err=1
conn_err=9 msg_append_err=0 unreliable-errno=0
nbytes-sent=22781160 compress-ratio=82.1%
rate in last 5sec, 30sec, 60sec
msg/sec: 6.0 6.0 5.9
log/sec: 280.4 290.2 285.2
```

The remote analyzer with this feature displays received compressed forwarded logs in `diagnose test application oftpd 7`.

### To view received compressed logs:

1. In the FortiAnalyzer CLI, enter the following command:

```
diagnose test application oftpd 7
```

The output will include information about received compressed logs within the *log-forward gen2 stats* section.

```
FAZVM64 # diagnose test application oftpd 7
Reliable logging stats:
  log=547 log(>4k)=36
Reliable log-forward stats:
  log=0 log(>4k)=0 reg=0 ack=0 ack_back=0 thr=0 optcode_err=0
Reliable log-forward gen2 stats:
Connections:
  From FAZ-VMTM20009184 @ 10.2.125.245 sig.745f02f721e21529 Connected 5m22.181s
  ago
  Pos=1610387635.768239362.24429530.7 tlvm-ver=2 last_rcv=1610387153 n_
  flushed=2457 n_compressed=2457
Stats:
  add=1 del=0 replace=0
  inactive=0 expired=0
Errors:
  conn=0 conn_info=0 discard=0
  epoll.add=0 epoll.del=0
  rcv_tlvm=0 rcv_oversize=0 parse_msg=0 build_resp=0
Internal log-forward stats:
  queued=0 (max=2048) update=757 (now=759)
errors
  fortilogd-not-running=0 no-init=0 socket=0 no-recv=0 unknown=0
Internal-forward stats by source:
  dev-nonreliable : 0
  fwd-reliable : 2457
  fwd-nonreliable : 0
  dev-batch-upload : 0
```



```

fct-batch-upload : 0
dev-reliable : 0
fwd-reliable-unencrypted : 0
fwd-ha-isync : 0
fwd-ha-isync-ack : 0
dev-reliable-encrypted : 547
fna-upload : 0
faz-appvt : 0
fct-siem : 0
unknown : 0

```

## Per-device log receiving rate limit

This feature adds the ability to set log rate limit per device to pause log insertion when the configured limit is exceeded. This is to prevent misconfigured devices from flooding FortiAnalyzer with unwanted data.

### To configure per-device log receiving rates:

1. Go to the FortiAnalyzer CLI and use the following commands to see that log receiving rate limits are not currently set:

```

FAZ3000F # config system log ratelimit
(ratelimit)# get
mode : disable
(ratelimit)#

```

Enter the following command to view the current logging rates for each device:

```

AZ3000F # diagnose test application fortilogd 17
# device 1_minute 10_minute rate-limit dropped

```

```

-----
1 FGT60E9982377487 34906.10 11800.36 0 0
2 FG800D3915800008 1988.57 690.44 0 0
3 FGHA000947503766_CID 0.00 0.00 0 0
4 FGT51E3U16002689 0.47 0.17 0 0
5 FWF61FTK19000247 45387.15 15514.16 0 0
6 FAC-VM0000000000 0.00 0.00 0 0
7 SYSLOG-AC105101 0.00 0.00 0 0
8 FG140P3G13800040 12895.43 4495.17 0 0
9 FGT60E9982377480 34906.83 11805.59 0 0
10 FG280P4614800414 0.07 0.01 0 0
11 FG101FTK19006708 9785.22 3177.97 0 0
12 FL-3KF3R16000142 0.00 0.00 0 0
13 FL3K5F3M15000004 0.02 0.01 0 0
14 FGT40FTK20025663 19553.53 7087.56 0 0
15 System 159423.38 54571.44 0 0

```

2. In the CLI, use the following commands to set the log receiving rate limit to manual and configure a new default rate limit:

```

FAZ3000F # config system log ratelimit
(ratelimit)# show
config system log ratelimit
set mode manual
set device-ratelimit-default 1000
end

```

Enter the following command to view the updated default rate limit applied to logging devices:

```

FAZ3000F # diagnose test application fortilogd 17
# device 1_minute 10_minute rate-limit dropped

```

```

-----
1 FGT60E9982377487 1000.18 20781.08 1000 6680050
2 FG800D3915800008 1000.82 1385.01 1000 210858
3 FGHA000947503766_CID 0.00 0.00 1000 0
4 FGT51E3U16002689 0.45 0.42 1000 0
5 FWF61FTK19000247 1000.48 27342.83 1000 6779154
6 FAC-VM0000000000 0.00 0.00 1000 0
7 SYSLOG-AC105101 0.00 0.00 1000 0
8 FG140P3G13800040 1001.70 7753.74 1000 484191
9 FGT60E9982377480 1000.03 20778.19 1000 6680607
10 FG280P4614800414 0.07 0.05 1000 0
11 FG101FTK19006708 1000.52 5558.64 1000 1253065
12 FL-3KF3R16000142 0.00 0.00 1000 0
13 FL3K5F3M15000004 0.03 0.02 1000 0
14 FGT40FTK20025663 1001.62 12567.55 1000 3140384
15 System 7005.90 96167.54 42000 25228309

```

**3. In the CLI, use the following commands to configure a per-device log rate limit for your devices.**

In this example, the FortiGate device is configured with a 2000 rate limit and FortiWiFi 61F devices are configured with a 1500 rate limit using wildcard support.

```

FAZ3000F # config system log ratelimit
(ratelimit)# show
config system log ratelimit
set mode manual
config device
edit 1
set device "FGT60E9982377480"
set ratelimit 2000
next
edit 2
set device "FWF61F*"
set ratelimit 1500
next
end
set device-ratelimit-default 1000
end

```

Enter the following command to view the updated log rate limits:

```

FAZ3000F # diagnose test application fortilogd 17
# device 1_minute 10_minute rate-limit dropped
-----
1 FGT60E9982377487 1000.12 1000.18 1000 128460813
2 FG800D3915800008 812.20 882.80 1000 3990480
3 FGT51E3U16002689 0.40 0.58 1000 0
4 FWF61FTK19000247 1501.23 1369.88 1500 48970326
5 FAC-VM0000000000 0.00 0.00 1000 0
6 SYSLOG-AC105101 0.00 0.00 1000 0
7 FG140P3G13800040 0.00 704.49 1000 2673191
8 FGT60E9982377480 2000.07 1100.19 2000 128984024
9 FG280P4614800414 0.07 0.06 1000 0
10 FG101FTK19006708 1000.92 914.34 1000 24125577
11 FL-3KF3R16000142 0.00 0.00 1000 0
12 FL3K5F3M15000004 0.02 0.02 1000 0
13 FGT40FTK20025663 1001.30 917.09 1000 34486937
14 System 7316.32 6889.65 42000 371691348

```

**4. Check the alert messages in widget Alert Message console to view messages about when log rate limits are exceed and logs are dropped:**

Time Message

```
Feb 25, 09:36:08 Device FGT60E0000000299 logs dropped due to exceed configured rate-
limit 60 logs/sec.
Feb 25, 09:36:08 Device FGT60E0000000435 logs dropped due to exceed configured rate-
limit 60 logs/sec.
Feb 25, 09:36:08 Device FGT60E0000000260 logs dropped due to exceed configured rate-
limit 60 logs/sec.
Feb 25, 09:36:07 Device FGT40FTK20025663 log-rate limited due to exceed configured
rate-limit 1000 logs/sec.
Feb 25, 09:36:07 Device FG101FTK19006708 log-rate limited due to exceed configured
rate-limit 1000 logs/sec.
```

This information is also available in local event logs:

```
id=6933257507120873474 itime=2021-02-25 09:40:08 euid=1 epid=1 dsteuid=1 dstepid=1
log_id=0030039002 subtype=logging type=event level=alert time=09:40:08
date=2021-02-25 action=alert msg=Device FGT60E0000000121 logs dropped due to
exceed configured rate-limit 60 logs/sec. desc=Log rate limit alert devid=FL-
3KF3R16000142 devname=FL-3KF3R16000142 dtime=2021-02-25 09:40:08 itime_
t=1614274808
id=6933257502825906182 itime=2021-02-25 09:40:07 euid=1 epid=1 dsteuid=1 dstepid=1
log_id=0030039002 subtype=logging type=event level=alert time=09:40:07
date=2021-02-25 action=alert msg=Device FWF61FTK19000247 log-rate limited due to
exceed configured rate-limit 1500 logs/sec. desc=Log rate limit alert devid=FL-
3KF3R16000142 devname=FL-3KF3R16000142 dtime=2021-02-25 09:40:07 itime_
t=1614274807
```

## Mask user data in log forwarder

FortiAnalyzer includes an option to mask user privacy data when forwarding logs to a remote server in one of the supported types: FortiAnalyzer, Syslog, or CEF.

## To configure data masking in log forwarding:

1. Go to *System Settings > Log Forwarding*, and configure a new or existing log forwarding profile.
2. Set the *Enable Masking* toggle to the *ON* position.  
Select the fields to be masked in *Masking Data Fields*, and create a *Data Mask Key*.

**Edit Log Forwarding**

Name: faz-248

Status: ☒ ON

Remote Server Type: ☒ FortiAnalyzer ☐ Syslog ☐ Common Event Format(CEF)

Server IP: 10.2.125.248

Server Port: 514

Reliable Connection: ☒ ON

---

**Log Forwarding Filters**

Device Filters: FG100D3G00002900, FG100D3G00002901

Log Filters: ☐ OFF

Enable Exclusions: ☐ OFF

Enable Masking: ☒ ON

Masking Data Fields: ☒ User ☐ Source IP ☐ Source Name ☒ Source MAC ☐ Destination IP ☐ Destination Name ☐ Email ☐ Message ☐ Domain

Data Mask Key: \*\*\*\*\*

OK Cancel

3. Click *OK* to save the log forwarding profile.  
The remote server will receive logs with the selected field values masked.

2 Devices selected

| #  | ▼ Date/Time | Device ID        | Action          | Unauthenticated User | Source                                   | User                   | Destination IP  | Service | Applicati |
|----|-------------|------------------|-----------------|----------------------|------------------------------------------|------------------------|-----------------|---------|-----------|
| 1  | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.182) | qKrd3PWlQxd5WOP6f8q... | 172.17.93.255   | 137/udp | 137/L...  |
| 2  | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.182) | qKrd3PWlQxd5WOP6f8q... | 172.17.93.255   | 137/udp | 137/L...  |
| 3  | 11:49:00    | FG100D3G00002900 |                 |                      | qKrd3PWlQxd5WOP6f8qwZw== (192.168.3.4)   | qKrd3PWlQxd5WOP6f8q... | 162.250.145.46  | NTP     | NTP       |
| 4  | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.146) | qKrd3PWlQxd5WOP6f8q... | 255.255.255.255 | DHCP    | DHCF      |
| 5  | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.146) | qKrd3PWlQxd5WOP6f8q... | 255.255.255.255 | DHCP    | DHCF      |
| 6  | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.144) | qKrd3PWlQxd5WOP6f8q... | 255.255.255.255 | DHCP    | DHCF      |
| 7  | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.144) | qKrd3PWlQxd5WOP6f8q... | 255.255.255.255 | DHCP    | DHCF      |
| 8  | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.252) | qKrd3PWlQxd5WOP6f8q... | 255.255.255.255 | DHCP    | DHCF      |
| 9  | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.252) | qKrd3PWlQxd5WOP6f8q... | 255.255.255.255 | DHCP    | DHCF      |
| 10 | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.3)   | qKrd3PWlQxd5WOP6f8q... | 255.255.255.255 | DHCP    | DHCF      |
| 11 | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.3)   | qKrd3PWlQxd5WOP6f8q... | 255.255.255.255 | DHCP    | DHCF      |
| 12 | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.171) | qKrd3PWlQxd5WOP6f8q... | 172.17.93.255   | 138/udp | 138/L...  |
| 13 | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.171) | qKrd3PWlQxd5WOP6f8q... | 172.17.93.255   | 138/udp | 138/L...  |
| 14 | 11:49:00    | FG100D3G00002900 | Policy viola... |                      | qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.171) | qKrd3PWlQxd5WOP6f8q... | 172.17.93.255   | 138/udp | 138/L...  |

100 items per page

Security Level: warning

Source: FG100D3G00002900

Device Name: FG100D3G00002900

Group: ZidRy4nPVp6EUBVH2Qw==

Interface: port1

Name: 172.17.93.200

Port: 626

Source: qKrd3PWlQxd5WOP6f8qwZw== (172.17.93.200)

User: qKrd3PWlQxd5WOP6f8qwZw==

Action: Policy violation

Firewall Action: deny

Per-IP Shaper: N/A

Policy ID: 0

Received Shaper Name: N/A

Sent Shaper Name: N/A

Duration: 5 seconds

Per-IP Shaper Bytes Discarded: n

General: Log ID: 7

Message: inspect\_ip\_check() check failed, drop

Session ID: 56795265

Virtual Domain: MTFDEV8101F

Destination: Country: Reserved

IP: 224.0.0.1

Interface: N/A

Name: 224.0.0.1

Port: 626

Application: Application: 626/udp

Application Category: Not Scanned

Protocol: 17

Service: 626/udp

Type: Sub Type: forward

Type: traffic

## To configure log field exclusion in log forwarding:

1. Go to *System Settings > Log Forwarding*, and configure a new or existing log forwarding profile.

- Set the *Enable Exclusions* toggle to the *ON* position.  
Add at least one log field to exclude.

- Click *OK* to save the log forwarding profile.  
The remote server will receive logs with the selected log field removed.  
Log field exclusion will occur even when the same log field is also configured to be masked using data masking.

## Configuring log field masking and exclusions in the CLI

The `log-field-exclusion-status` command was added to configure log field exclusions in the CLI.

The `log-masking-status` command was added to configure log field masking in the CLI.

The following is an example of the CLI used to configure log masking and exclusions:

```
config system log-forward
  edit 1
    set mode forwarding
    set fwd-max-delay realtime
    set server-name "faz-248"
    set server-ip "10.2.125.248"
    set fwd-reliable enable
    set sync-metadata sf-topology interface-role device endusr-avatar
    config device-filter
      edit 1
        set device "FG100D3G00002900"
      next
      edit 2
        set device "FG100D3G00002901"
      next
    end
    set signature 5899086158772996474
    set log-field-exclusion-status enable
    config log-field-exclusion
      edit 1
        set field-list "unauthuser"
      next
      edit 2
```

```

set log-type ANY-TYPE
set field-list "srcip"
next
end
set log-masking-status enable
set log-masking-fields user srcmac
set log-masking-key ENC
MTI0MDIwNDAxNDU4MzE3Nwt6SkhHfPMpmk5BN3cthOBoZwEvkj1BLEzBvUk89vcWnE006zRVadjlp9
dPTJ8fw3svp1FF2uiPb5h6iN+Y0Y/be4sGO0JlTYVuMoyz5Od6xgmAFnG1M7F3QLNpXMP1COjD8MNR
Ito
next
end

```

## FortiEDR Central Manager logging

FortiEDR Central Manager can send its logs in Syslog format to FortiAnalyzer and the FortiAnalyzer parses the logs and inserts them into its SIEM database for event correlation and reporting.

To view FortiEDR logs in the Fabric log view:

1. FortiAnalyzer can collect FortiEDR Central Manager logs in Syslog.

The screenshot shows the FortiAnalyzer Log View interface. The left sidebar has a tree view with 'Fabric' expanded, showing 'FortiAnalyzer' and 'Syslog'. The 'Syslog' option is selected. The main pane displays a table of logs with columns: #, Date/Time, Device ID, Level, and Message. The logs are filtered for 'All Syslog' and show a list of events from 10:00:41 to 10:14:53, all with a 'notice' level. The messages are truncated, showing a URL and a message type.

| #  | Date/Time | Device ID       | Level  | Message                                                                                                 |
|----|-----------|-----------------|--------|---------------------------------------------------------------------------------------------------------|
| 1  | 10:00:41  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:00:41.158Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 2  | 10:01:34  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:01:34.016Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 3  | 10:01:38  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:01:38.369Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 4  | 10:02:01  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:02:01.762Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 5  | 10:05:28  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:05:28.451Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 6  | 10:14:50  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:14:50.271Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 7  | 10:14:50  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:14:50.766Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 8  | 10:14:51  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:14:51.264Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 9  | 10:14:51  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:14:51.764Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 10 | 10:14:52  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:14:52.265Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 11 | 10:14:52  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:14:52.896Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 12 | 10:14:53  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:14:53.407Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |
| 13 | 10:14:53  | SYSLOG-68C766C6 | notice | 1 2021-02-03T18:14:53.893Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Orga... |

Before this enhancement, FortiAnalyzer uses the syslog parser to parse FortiEDR Central Manager logs in SIEM.

The screenshot shows the FortiAnalyzer Log View interface with the 'Detailed Information' tab selected. It displays a list of log entries with their full details, including timestamps, device IDs, and message content. The first entry is highlighted, showing a message about a security event. The bottom of the screen shows a summary of the logs for the selected time range.

| # | Detailed Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | itime=2021-01-20 20:15:52 epid=1 uid=1 data_parsename=Syslog parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=Syslog data_timestamp=0 event_message=1 2021-01-21T04:15:52.635Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Organization: ensilofordev;Date and Time: 20-Jan-2021, 23:15:52;Sub-system: Events;User Name: roy;Description: 1 event was marked as read event_type-generic itime_t=1611202552                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2 | itime=2021-01-20 20:55:25 epid=1 uid=1 data_parsename=Syslog parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=Syslog data_timestamp=0 event_message=1 2021-01-21T04:55:25.692Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Organization: ensilofordev;Date and Time: 20-Jan-2021, 23:55:25;Sub-system: System;User Name: roy;Description: System logout (Internal) event_type-generic itime_t=1611204925                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 3 | itime=2021-01-20 22:46:11 epid=1 uid=1 data_parsename=Syslog parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=Syslog data_timestamp=0 event_message=1 2021-01-21T06:43:07.000Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Security Event;Organization: ensilofordev;Organization ID: 1;Event ID: 4461197;Raw Data ID: 1741136096;Device Name: ensw-lap-152;Operating System: Windows 10 Pro;Process Name: powershell.exe;Process Path: DeviceHarddiskVolume3\Windows\System32\WindowsPowerShell\1.0\powershell.exe;Process Type: 64bit;Severity: High;Classification: Inconclusive;Destination: File Access;First Seen: 21-Jan-2021, 01:43:07;Last Seen: 21-Jan-2021, 01:43:07;Action: Blocked;Count: 1;Certificate: yes;Rules List: Disk encryption attempt detected - Suspicious full disk encryption was detected;Users: ENSILOshanih;MAC Address: 08-BE-AC-20-D6-30-74-70-FD-BC-59-17-10-65-30-6D-C9-BB;Script: \$Res;Script Path: N/A;Autonomous System: N/A;Country: N/A;Process Hash: F43D9BB316E30AE1A3494AC5B0624F6BEA1BF054;Source IP: 10.0.0.1 event_type-generic itime_t=1611211571 |
| 4 | itime=2021-01-20 23:02:42 epid=1 uid=1 data_parsename=Syslog parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=Syslog data_timestamp=0 event_message=1 2021-01-21T07:02:42.5288Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Organization: ensilofordev;Date and Time: 21-Jan-2021, 02:02:39;Sub-system: Events;User Name: FortinetCloudServices;Description: Classification was changed to 'Safe' for event 4461567 event_type-generic itime_t=1611212559                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 5 | itime=2021-01-20 23:02:40 epid=1 uid=1 data_parsename=Syslog parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=Syslog data_timestamp=0 event_message=1 2021-01-21T07:02:39.944Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Organization: ensilofordev;Date and Time: 21-Jan-2021, 02:02:39;Sub-system: Events;User Name: FortinetCloudServices;Description: Classification was changed to 'Safe' for event 4461557 event_type-generic itime_t=1611212560                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 6 | itime=2021-01-20 23:02:42 epid=1 uid=1 data_parsename=Syslog parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=Syslog data_timestamp=0 event_message=1 2021-01-21T07:02:42.693Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Organization: ensilofordev;Date and Time: 21-Jan-2021, 02:02:42;Sub-system: Events;User Name: FortinetCloudServices;Description: Classification was changed to 'Safe' for event 4461576 event_type-generic itime_t=1611212562                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 7 | itime=2021-01-20 23:02:45 epid=1 uid=1 data_parsename=Syslog parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=Syslog data_timestamp=0 event_message=1 2021-01-21T07:02:51.995Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Organization: ensilofordev;Date and Time: 21-Jan-2021, 02:02:51;Sub-system: Events;User Name: FortinetCloudServices;Description: Classification was changed to 'Safe' for event 4461540 event_type-generic itime_t=1611212565                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 8 | itime=2021-01-20 23:02:52 epid=1 uid=1 data_parsename=Syslog parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=Syslog data_timestamp=0 event_message=1 2021-01-21T07:02:51.995Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Organization: ensilofordev;Date and Time: 21-Jan-2021, 02:02:51;Sub-system: Events;User Name: FortinetCloudServices;Description: Classification was changed to 'Safe' for event 4461548 event_type-generic itime_t=1611212572                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 9 | itime=2021-01-20 23:11:08 epid=1 uid=1 data_parsename=Syslog parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=Syslog data_timestamp=0 event_message=1 2021-01-21T07:11:08.000Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit;Organization: ensilofordev;Date and Time: 21-Jan-2021, 02:11:08;Sub-system: Events;User Name: FortinetCloudServices;Description: Classification was changed to 'Safe' for event 4461548 event_type-generic itime_t=1611212572                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Total logs for analytics: 15 days 16 hours. 100 Items per page 1 2 3 4 5 > 0.007 Second

FortiEDR Central Manager log messages and types did not display properly in the Fabric log view.

| #  | ▲ Date/Time | Data Source ID | Event Message                                                                                                                        | Event Type | Event Severity |
|----|-------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------|------------|----------------|
| 1  | 01-20 20:15 | SYSLOG-68C...  | 1 2021-01-21T04:15:52.635Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 2  | 01-20 20:55 | SYSLOG-68C...  | 1 2021-01-21T04:55:25.692Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 3  | 01-20 22:46 | SYSLOG-68C...  | 1 2021-01-21T06:43:07.000Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Security Event; Organization: ensilofor... | generic    |                |
| 4  | 01-20 23:02 | SYSLOG-68C...  | 1 2021-01-21T07:02:39.510Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 5  | 01-20 23:02 | SYSLOG-68C...  | 1 2021-01-21T07:02:39.944Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 6  | 01-20 23:02 | SYSLOG-68C...  | 1 2021-01-21T07:02:42.693Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 7  | 01-20 23:02 | SYSLOG-68C...  | 1 2021-01-21T07:02:45.288Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 8  | 01-20 23:02 | SYSLOG-68C...  | 1 2021-01-21T07:02:51.995Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 9  | 01-20 23:11 | SYSLOG-68C...  | 1 2021-01-21T07:11:08.707Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 10 | 01-20 23:11 | SYSLOG-68C...  | 1 2021-01-21T07:11:14.930Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 11 | 01-20 23:11 | SYSLOG-68C...  | 1 2021-01-21T07:11:33.200Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 12 | 01-20 23:11 | SYSLOG-68C...  | 1 2021-01-21T07:11:49.834Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 13 | 01-20 23:12 | SYSLOG-68C...  | 1 2021-01-21T07:12:43.364Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 14 | 01-20 23:19 | SYSLOG-68C...  | 1 2021-01-21T07:19:53.500Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 15 | 01-20 23:34 | SYSLOG-68C...  | 1 2021-01-21T07:34:00.463Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 16 | 01-20 23:35 | SYSLOG-68C...  | 1 2021-01-21T07:35:28.542Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 17 | 01-20 23:47 | SYSLOG-68C...  | 1 2021-01-21T07:47:19.604Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 18 | 01-20 23:47 | SYSLOG-68C...  | 1 2021-01-21T07:47:22.172Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 19 | 01-20 23:50 | SYSLOG-68C...  | 1 2021-01-21T07:50:53.429Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 20 | 01-21 00:15 | SYSLOG-68C...  | 1 2021-01-21T08:15:33.202Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 21 | 01-21 00:27 | SYSLOG-68C...  | 1 2021-01-21T08:27:47.002Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 22 | 01-21 01:17 | SYSLOG-68C...  | 1 2021-01-21T09:17:27.702Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 23 | 01-21 02:02 | SYSLOG-68C...  | 1 2021-01-21T10:02:02.550Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 24 | 01-21 02:02 | SYSLOG-68C...  | 1 2021-01-21T10:02:54.762Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |
| 25 | 01-21 02:09 | SYSLOG-68C...  | 1 2021-01-21T10:09:45.916Z https://nsloeng.console.ensilo.com/ enSilo - - - Message Type: Audit; Organization: ensilofordev; Date... | generic    |                |

## 2. After this enhancement, FortiAnalyzer includes a FortiEDR parser in the SIEM to parse FortiEDR Central Manager logs.

| #  | Detailed Information                                                                                                                                                                                                                                                                                                                                          |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | itime=2021-02-03 10:41:02 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612377661 event_message=System logout (Internal) event_type=Audit src_domain=InfoSecTesting user_name=whitehatsecDast itime_t=1612377662                                                                         |
| 2  | itime=2021-02-03 10:20:10 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376410 event_message=System login for Organization http://whsec.us/rf.php failed due to an incorrect user name or password event_type=Audit src_domain=ensilofordev itime_t=1612376410                        |
| 3  | itime=2021-02-03 10:20:10 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376410 event_message=System login for Organization whsec.us/rf.php failed due to an incorrect user name or password event_type=Audit src_domain=ensilofordev itime_t=1612376410                               |
| 4  | itime=2021-02-03 10:20:09 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376409 event_message=System login for Organization http://whsec.us/rf.php? failed due to an incorrect user name or password event_type=Audit src_domain=ensilofordev itime_t=1612376409                       |
| 5  | itime=2021-02-03 10:20:09 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376409 event_message=System login for Organization php://filter/resource=http://whsec.us/rf.php? failed due to an incorrect user name or password event_type=Audit src_domain=ensilofordev itime_t=1612376409 |
| 6  | itime=2021-02-03 10:19:54 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376394 event_message=System login for Organization data://text/plain event_type=Audit src_domain=ensilofordev itime_t=1612376394                                                                              |
| 7  | itime=2021-02-03 10:19:53 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376393 event_message=System login failed event_type=Audit src_domain=ensilofordev itime_t=1612376393                                                                                                          |
| 8  | itime=2021-02-03 10:19:53 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376393 event_message=System login failed event_type=Audit src_domain=ensilofordev itime_t=1612376393                                                                                                          |
| 9  | itime=2021-02-03 10:19:52 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376392 event_message=System login failed event_type=Audit src_domain=ensilofordev user_name=http://whsec.us/rf.php itime_t=1612376392                                                                         |
| 10 | itime=2021-02-03 10:19:52 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376392 event_message=System login failed event_type=Audit src_domain=ensilofordev user_name=whsec.us/rf.php itime_t=1612376392                                                                                |
| 11 | itime=2021-02-03 10:19:51 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376391 event_message=System login failed event_type=Audit src_domain=ensilofordev itime_t=1612376391                                                                                                          |
| 12 | itime=2021-02-03 10:19:51 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376391 event_message=System login failed event_type=Audit src_domain=ensilofordev itime_t=1612376391                                                                                                          |
| 13 | itime=2021-02-03 10:19:50 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376390 event_message=System login failed event_type=Audit src_domain=ensilofordev user_name=http://whsec.us/rf.php? itime_t=1612376390                                                                        |
| 14 | itime=2021-02-03 10:19:50 epid=1 uid=1 data_parsename=FortiEDR parser data_sourceid=SYSLOG-68C766C6 data_sourcetype=FortiEDR data_timestamp=1612376390 event_message=System login failed event_type=Audit src_domain=ensilofordev user_name=http://whsec.us/rf.php? itime_t=1612376390                                                                        |

FortiAnalyzer can display FortiEDR Central Manager logs properly in the Fabric.

| #  | Date/Time | Data Source ID | Event Message                                                                                                                | Event Type | Event Severity |
|----|-----------|----------------|------------------------------------------------------------------------------------------------------------------------------|------------|----------------|
| 1  | 10:41:02  | SYSLOG-68C...  | System logout (Internal)                                                                                                     | Audit      |                |
| 2  | 10:20:10  | SYSLOG-68C...  | System login for Organization http://whsec.us/rf.php failed due to an incorrect user name or password                        | Audit      |                |
| 3  | 10:20:10  | SYSLOG-68C...  | System login for Organization whsec.us/rf.php failed due to an incorrect user name or password                               | Audit      |                |
| 4  | 10:20:09  | SYSLOG-68C...  | System login for Organization http://whsec.us/rf.php? failed due to an incorrect user name or password                       | Audit      |                |
| 5  | 10:20:09  | SYSLOG-68C...  | System login for Organization php://filter/resource=http://whsec.us/rf.php? failed due to an incorrect user name or password | Audit      |                |
| 6  | 10:19:54  | SYSLOG-68C...  | System login for Organization data://text/plain                                                                              | Audit      |                |
| 7  | 10:19:53  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 8  | 10:19:53  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 9  | 10:19:52  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 10 | 10:19:52  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 11 | 10:19:51  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 12 | 10:19:51  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 13 | 10:19:50  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 14 | 10:19:50  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 15 | 10:19:49  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 16 | 10:19:49  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 17 | 10:19:31  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 18 | 10:19:31  | SYSLOG-68C...  | System login for Organization <% whs=21705 %>whscheck<%= whs.to_s %> failed due to an incorrect user name or password        | Audit      |                |
| 19 | 10:19:30  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 20 | 10:19:30  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 21 | 10:19:29  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 22 | 10:19:29  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 23 | 10:19:28  | SYSLOG-68C...  | System login failed                                                                                                          | Audit      |                |
| 24 | 10:19:28  | SYSLOG-68C...  | System login for Organization failed due to an incorrect user name or password                                               | Audit      |                |
| 25 | 10:19:27  | SYSLOG-68C...  | System login for Organization failed due to an incorrect user name or password                                               | Audit      |                |

## FortiAI logging on FortiAnalyzer - 7.0.1

Starting in FortiAnalyzer 7.0.1, you can configure FortiAnalyzer to accept logs from a FortiAI device for use in the following ways:

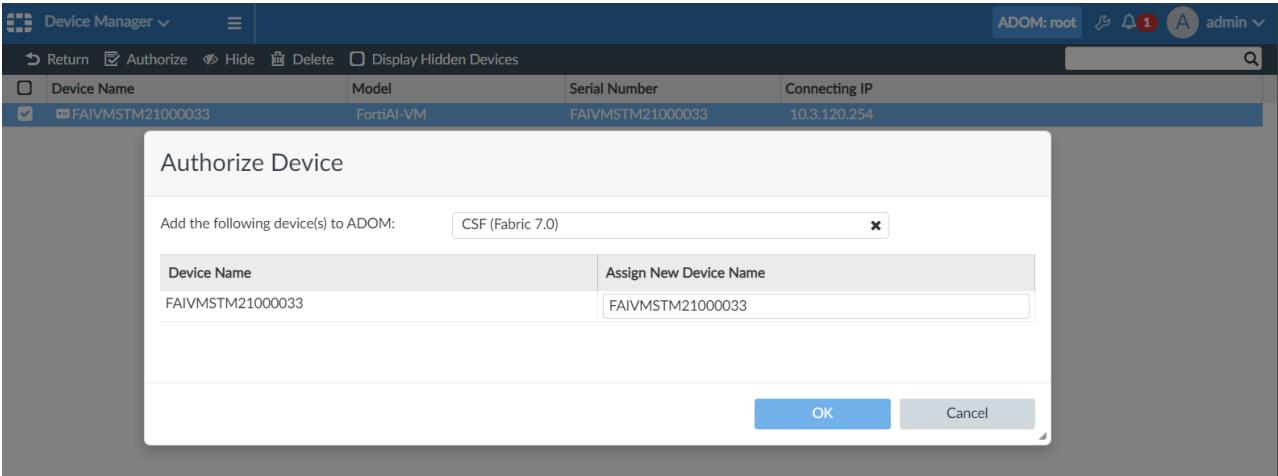
- FortiAnalyzer can recognize FortiAI devices.
- FortiAI logs can be stored in Fabric ADOM.
- FortiAI can be viewed in LogView.
- FortiAI Device Type and Log Types are available in event handlers and report data sets.

### To add a FortiAI device to FortiAnalyzer:

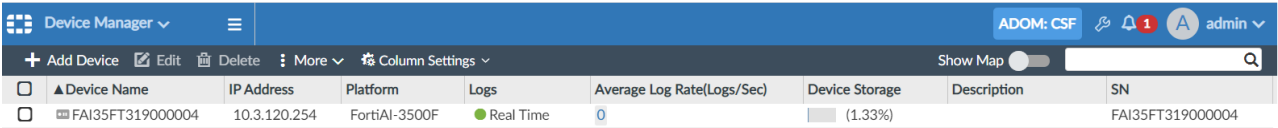
1. On FortiAnalyzer, ensure you are in the correct ADOM.
2. Go to *Device Manager* and add the FortiAI device.  
Previously, FortiAnalyzer could not recognize FortiAI devices. In 7.0.1 and later, FortiAnalyzer is able to recognize



the FortiAI device and will display it in the *Unauthorized Device* list once added.



3. Select *Unauthorized Devices* and authorize the FortiAI device.  
When the FortiAI device is authorized on FortiAnalyzer, it is listed in the FortiAnalyzer *Device Manager* with information including its device name, IP, serial number, logging status, etc.



### To view FortiAI logs in FortiAnalyzer:

1. On FortiAnalyzer, ensure you are in the correct ADOM.
2. Go to **Log View > FortiAI**.

There is a new *FortiAI* log type created for the FortiAI device. When FortiAI logs are received, they are displayed in *Log View*.

| #  | Date/Time   | Device ID        | Type  | Sub Type | Level       | User | Status  |
|----|-------------|------------------|-------|----------|-------------|------|---------|
| 1  | 06-10 22:11 | FAI35FT319000004 | event |          | information |      | success |
| 2  | 06-10 22:48 | FAI35FT319000004 | event |          | information |      | success |
| 3  | 06-10 23:24 | FAI35FT319000004 | event |          | information |      | success |
| 4  | 00:00:44    | FAI35FT319000004 | event |          | information |      | success |
| 5  | 00:36:59    | FAI35FT319000004 | event |          | information |      | success |
| 6  | 01:13:14    | FAI35FT319000004 | event |          | information |      | success |
| 7  | 01:49:29    | FAI35FT319000004 | event |          | information |      | success |
| 8  | 02:25:44    | FAI35FT319000004 | event |          | information |      | success |
| 9  | 03:01:59    | FAI35FT319000004 | event |          | information |      | success |
| 10 | 03:38:14    | FAI35FT319000004 | event |          | information |      | success |
| 11 | 03:38:15    | FAI35FT319000004 | event |          | information |      | success |
| 12 | 04:14:30    | FAI35FT319000004 | event |          | information |      | success |
| 13 | 05:08:37    | FAI35FT319000004 | event |          | information |      | success |
| 14 | 06:02:44    | FAI35FT319000004 | event |          | information |      | success |
| 15 | 06:56:51    | FAI35FT319000004 | event |          | information |      | success |
| 16 | 07:50:58    | FAI35FT319000004 | event |          | information |      | success |
| 17 | 08:45:05    | FAI35FT319000004 | event |          | information |      | success |
| 18 | 09:39:12    | FAI35FT319000004 | event |          | information |      | success |

Total logs for analytics: 1 day 17 hours. 50 Items per page. 1 page. 0.009 Second

3. Go to **Log View > Fabric**.

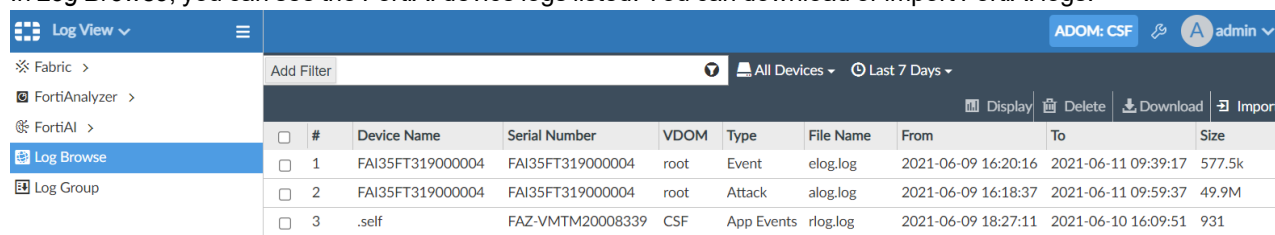
FortiAnalyzer adds a SIEM parser to FortiAI logs so that they can be viewed in the Fabric SIEM database correctly.

| #  | Date/Time | Data Source ID   | Event Type | Event Severity | Source IP     | Data Parser Name | Data Source Type |
|----|-----------|------------------|------------|----------------|---------------|------------------|------------------|
| 1  | 10:01:13  | FAI35FT319000004 | attack     | alert          |               | FortiAI parser   | FortiAI          |
| 2  | 10:01:12  | FAI35FT319000004 | attack     | alert          | 192.168.100.2 | FortiAI parser   | FortiAI          |
| 3  | 10:01:11  | FAI35FT319000004 | attack     | alert          |               | FortiAI parser   | FortiAI          |
| 4  | 10:01:10  | FAI35FT319000004 | attack     | alert          | 192.168.100.2 | FortiAI parser   | FortiAI          |
| 5  | 10:01:09  | FAI35FT319000004 | attack     | alert          |               | FortiAI parser   | FortiAI          |
| 6  | 10:01:08  | FAI35FT319000004 | attack     | alert          | 192.168.100.2 | FortiAI parser   | FortiAI          |
| 7  | 10:01:07  | FAI35FT319000004 | attack     | alert          |               | FortiAI parser   | FortiAI          |
| 8  | 10:01:06  | FAI35FT319000004 | attack     | alert          | 192.168.100.2 | FortiAI parser   | FortiAI          |
| 9  | 10:01:05  | FAI35FT319000004 | attack     | alert          |               | FortiAI parser   | FortiAI          |
| 10 | 10:01:04  | FAI35FT319000004 | attack     | alert          | 192.168.100.2 | FortiAI parser   | FortiAI          |
| 11 | 10:01:03  | FAI35FT319000004 | attack     | alert          |               | FortiAI parser   | FortiAI          |
| 12 | 10:01:02  | FAI35FT319000004 | attack     | alert          | 192.168.100.2 | FortiAI parser   | FortiAI          |
| 13 | 10:01:01  | FAI35FT319000004 | attack     | alert          |               | FortiAI parser   | FortiAI          |
| 14 | 10:01:00  | FAI35FT319000004 | attack     | alert          | 192.168.100.2 | FortiAI parser   | FortiAI          |
| 15 | 10:00:59  | FAI35FT319000004 | attack     | alert          |               | FortiAI parser   | FortiAI          |
| 16 | 10:00:58  | FAI35FT319000004 | attack     | alert          | 192.168.100.2 | FortiAI parser   | FortiAI          |
| 17 | 10:00:57  | FAI35FT319000004 | attack     | alert          |               | FortiAI parser   | FortiAI          |
| 18 | 10:00:56  | FAI35FT319000004 | attack     | alert          | 192.168.100.2 | FortiAI parser   | FortiAI          |

Total logs for analytics: 1 day 17 hours. 50 Items per page. 1 2 3 4 5 pages. 0.125 Second

#### 4. Go to *Log View > Log Browse*.

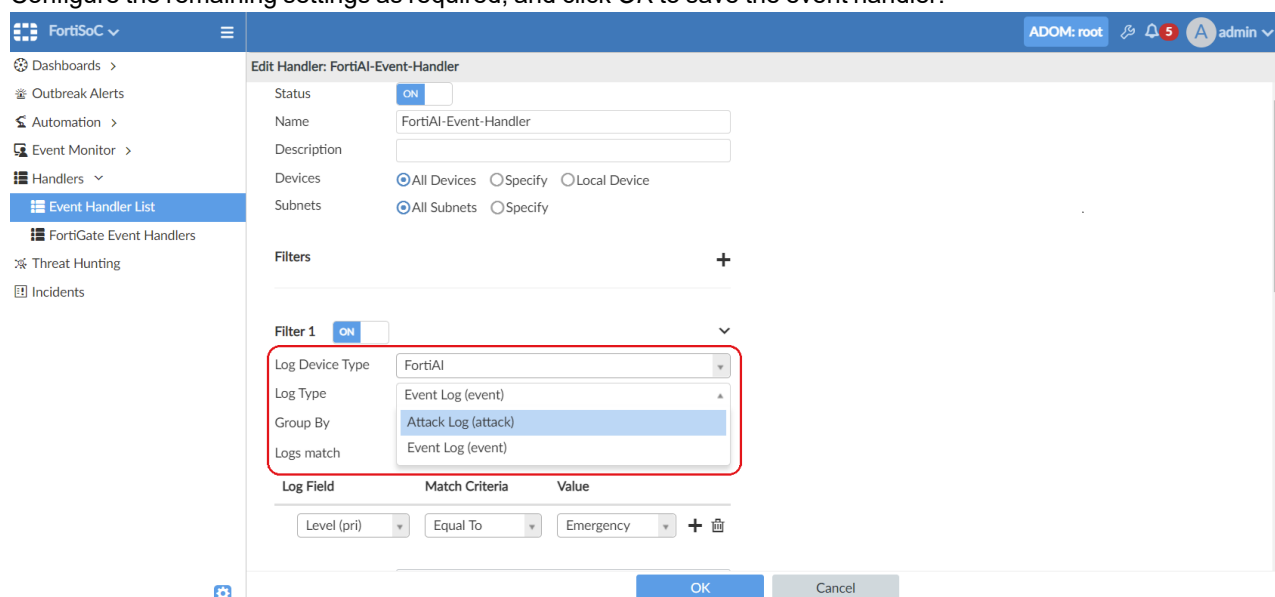
In *Log Browse*, you can see the FortiAI device logs listed. You can download or import FortiAI logs.



| # | Device Name      | Serial Number    | VDOM | Type       | File Name | From                | To                  | Size   |
|---|------------------|------------------|------|------------|-----------|---------------------|---------------------|--------|
| 1 | FAI35FT319000004 | FAI35FT319000004 | root | Event      | elog.log  | 2021-06-09 16:20:16 | 2021-06-11 09:39:17 | 577.5k |
| 2 | FAI35FT319000004 | FAI35FT319000004 | root | Attack     | alog.log  | 2021-06-09 16:18:37 | 2021-06-11 09:59:37 | 49.9M  |
| 3 | .self            | FAZ-VM20008339   | CSF  | App Events | rlog.log  | 2021-06-09 18:27:11 | 2021-06-10 16:09:51 | 931    |

#### To create a custom event handler using FortiAI logs:

1. Go to *FortiSoC > Handlers > Event Handler List*, and create a new event handler.
2. Enter a name for the event handler, for example *FortiAI-Event-Handler*.
3. Enable a filter, and select *FortiAI* as the *Log Device Type*.
4. In *Log type*, select a FortiAI log type.
5. Configure the remaining settings as required, and click *OK* to save the event handler.



**Edit Handler: FortiAI-Event-Handler**

Status: ☒ ON

Name: FortiAI-Event-Handler

Description:

Devices: ☒ All Devices ☐ Specify ☐ Local Device

Subnets: ☒ All Subnets ☐ Specify

Filters: +

Filter 1: ☒ ON

Log Device Type: FortiAI

Log Type: Event Log (event)

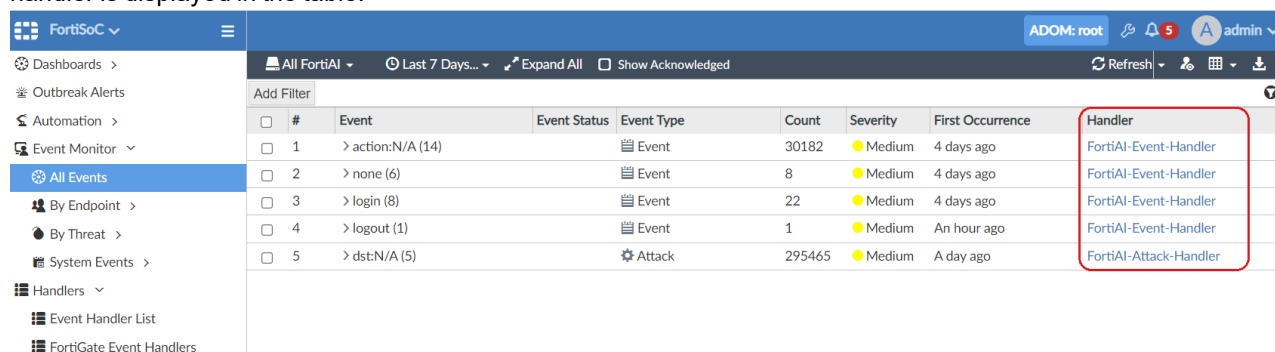
Group By: Attack Log (attack)

Logs match: Event Log (event)

Log Field: Level (pri) Match Criteria: Equal To Value: Emergency

OK Cancel

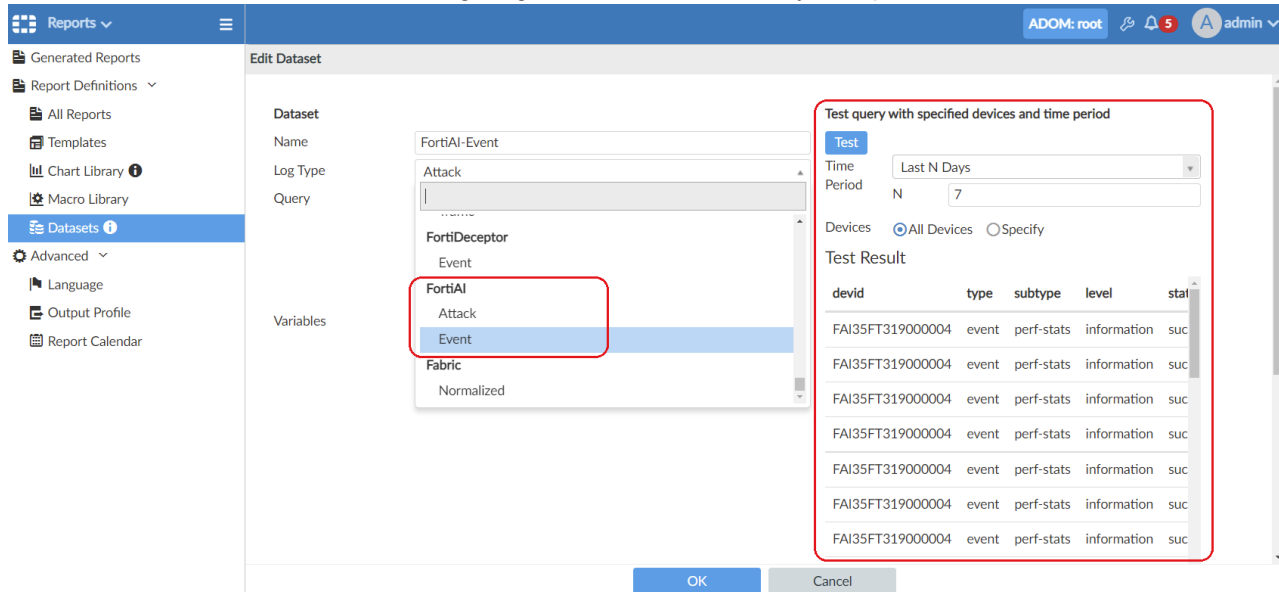
6. Events triggered by the event handler appear in *FortiSoC > Event Monitor > All Events*. The name of the event handler is displayed in the table.



| # | Event              | Event Status | Event Type | Count  | Severity | First Occurrence | Handler                |
|---|--------------------|--------------|------------|--------|----------|------------------|------------------------|
| 1 | > action: N/A (14) | Event        | Event      | 30182  | Medium   | 4 days ago       | FortiAI-Event-Handler  |
| 2 | > none (6)         | Event        | Event      | 8      | Medium   | 4 days ago       | FortiAI-Event-Handler  |
| 3 | > login (8)        | Event        | Event      | 22     | Medium   | 4 days ago       | FortiAI-Event-Handler  |
| 4 | > logout (1)       | Event        | Event      | 1      | Medium   | An hour ago      | FortiAI-Event-Handler  |
| 5 | > dst: N/A (5)     | Attack       | Attack     | 295465 | Medium   | A day ago        | FortiAI-Attack-Handler |

### To create a custom report using FortiAI logs:

1. Go to **Reports > Report Definitions > Datasets**, and create or edit a dataset.
2. Select a FortiAI log type in the Log Type dropdown.
3. Configure the remaining settings as required, and click **OK** to save the dataset.  
The dataset can now be used when configuring charts used in FortiAnalyzer reports.



## Log forwarding enhancement - 7.0.1

With this feature enhancement, FortiAnalyzer log-forward-cache-size can set more than 80% system reserved space helping to prevent log loss.

When the cache is full, the latest logs are kept and older logs are dropped.

### To configure the log forward cache size:

1. In the FortiAnalyzer CLI, enter the following commands to set the log forward cache size.  
In the following example, the cache size is set to 2000.  

```
config system global
set log-forward-cache-size 2000
Log-forward disk cache will be allocated from available disk quota and reserved space.
All logs currently in log-forward disk cache will be dropped.
Do you want to continue? (y/n)
```
2. In the CLI, enter the following command to see space usage:  

```
diagnose log device
Total Quota Summary:
Total Quota Adom Allocated Logfwd Allocated Available Allocate%
38140.9GB 32509.6GB 712.0GB(1000.0GB-288.0GB(reserved space)) 4919.3GB 87.1%
System Storage Summary:
Total Used Available Use%
38500.9GB 26634.6GB 11866.4GB 69.2%
Reserved space: 360.0GB ( 0.9% of total space, system reserved: 310.0GB,
FortiRecorder disk quota: 50.0GB)
```

## Reports

This section lists the new features added to FortiAnalyzer for reports:

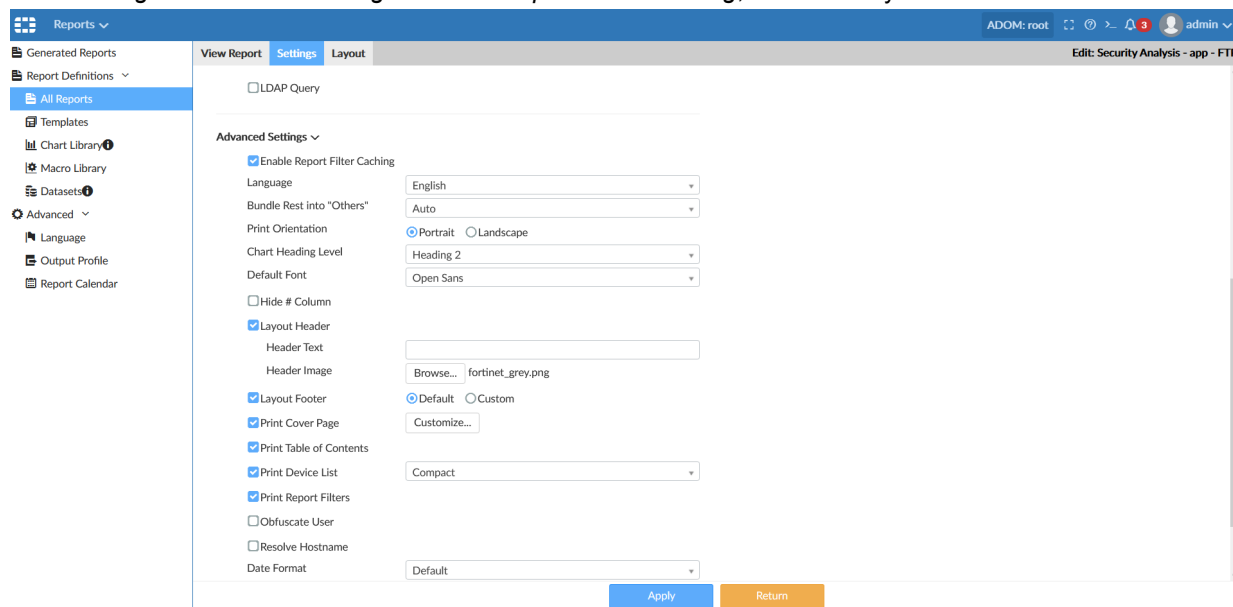
- Improved caching mechanism for reports on page 65
- FortiDeceptor report on page 68
- Central UEBA table for custom reporting and widgets on page 69
- FortiSandbox CTAP report on page 70
- Organize reports in folders on page 72
- Additional charts for SD-WAN reporting 7.0.1 on page 75

### Improved caching mechanism for reports

The report caching mechanism has been enhanced to improve processing speeds when generating multiple reports at the same time. When similar reports with different filters are processed at the same time, one hcache table is generated for all the reports in the queue.

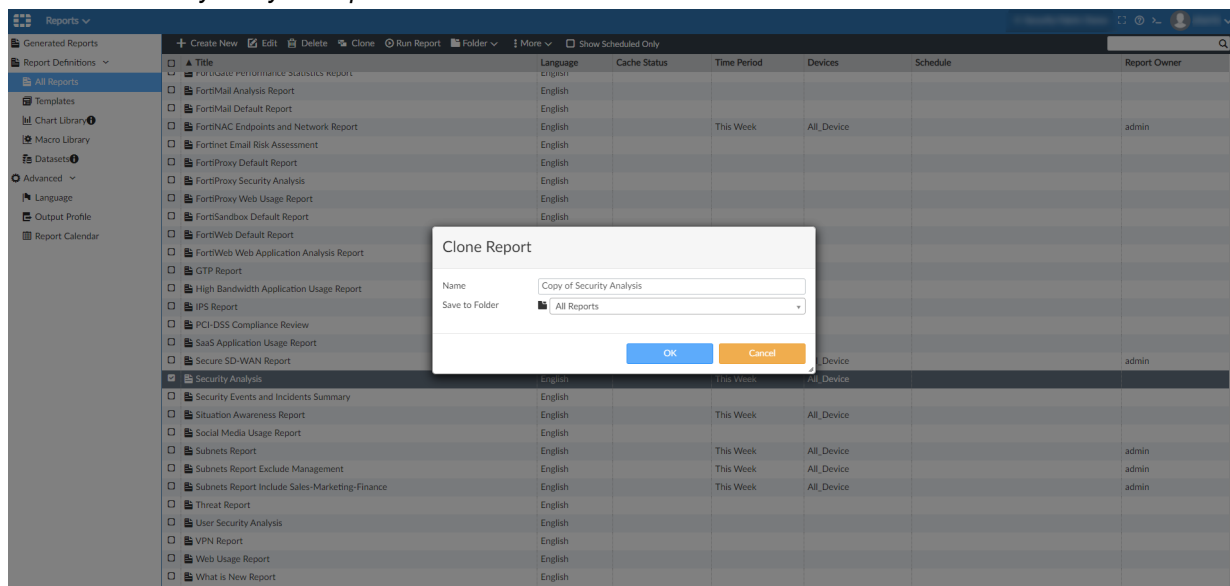
#### To run a report:

1. Go to *Reports > All Reports*, and select a report in the list.
2. Click *Settings > Advanced Settings*. *Enable Report Filter Caching*, is enabled by default.

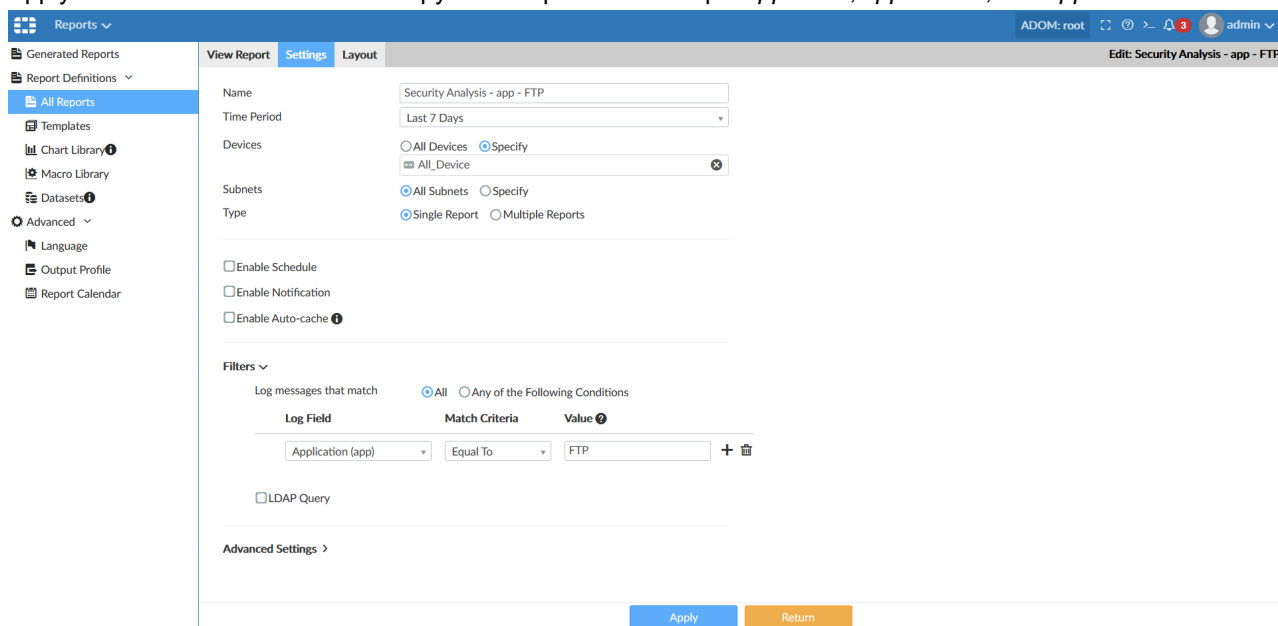


3. Click *Return*.

#### 4. Clone the *Security Analysis Report*.



#### 5. Apply different filter values to each copy of the report. For example *app=FTP*, *app=HTTP*, and *app=SSH*.



## 6. Select the cloned reports, and click *Run Report*.

| Report Name                              | Language | Cache Status | Time Period | Devices       | Schedule | Report Owner |
|------------------------------------------|----------|--------------|-------------|---------------|----------|--------------|
| FortiSandbox Default Report              | English  |              |             |               |          |              |
| FortiWeb Default Report                  | English  |              |             |               |          |              |
| FortiWeb Web Application Analysis Report | English  |              |             |               |          |              |
| GTP Report                               | English  |              |             |               |          |              |
| High Bandwidth Application Usage Report  | English  |              |             |               |          |              |
| IPS Report                               | English  |              |             |               |          |              |
| PCI-DSS Compliance Review                | English  |              |             |               |          |              |
| SaaS Application Usage Report            | English  |              |             |               |          |              |
| Secure SD-WAN Report                     | English  |              | Last 7 Days | All_FortiGate |          |              |
| Security Analysis                        | English  |              | Yesterday   | All_Device    |          |              |
| Security Analysis - app - FTP            | English  |              | Last 7 Days | All_Device    |          | admin        |
| Security Analysis - app - HTTP           | English  |              | Last 7 Days | All_Device    |          | admin        |
| Security Analysis - app - SSH            | English  |              | Last 7 Days | All_Device    |          | admin        |
| Security Events and Incidents Summary    | English  |              |             |               |          |              |
| Self-Harm and Risk Indicators Report     | English  |              |             |               |          |              |
| Situation Awareness Report               | English  |              |             |               |          |              |
| Social Media Usage Report                | English  |              |             |               |          |              |
| Threat Report                            | English  |              |             |               |          |              |
| User Security Analysis                   | English  |              |             |               |          |              |
| VPN Report                               | English  |              |             |               |          |              |
| Web Usage Report                         | English  |              |             |               |          |              |
| What is New Report                       | English  |              |             |               |          |              |
| WiFi Network Summary                     | English  |              |             |               |          |              |
| Wireless PCI Compliance                  | English  |              |             |               |          |              |

Before these enhancements were implemented, it would take minutes to process multiple reports at the same time.

| Report Name                                          | Format           | Time Range              | Devices      | Status  |
|------------------------------------------------------|------------------|-------------------------|--------------|---------|
| Today (3)                                            |                  |                         |              |         |
| Security Analysis - app - HTTP-2020-11-24-1145_14797 | HTML PDF XML CSV | 2020/11/16 - 2020/11/22 | >124 Devices | 05m 47s |
| Security Analysis - app - SSH-2020-11-24-1140_14795  | HTML PDF XML CSV | 2020/11/16 - 2020/11/22 | >124 Devices | 05m 44s |
| Security Analysis - app - FTP-2020-11-24-1133_14793  | HTML PDF XML CSV | 2020/11/16 - 2020/11/22 | >124 Devices | 06m 52s |

When *Enable Report Filter Caching* is enabled, it takes minutes to process the first report, while the processing time for subsequent reports is reduced to seconds.

The screenshot shows the 'Reports' section in FortiAnalyzer. The left sidebar contains 'Generated Reports', 'Report Definitions', 'All Reports', 'Templates', 'Chart Library', 'Macro Library', 'Datasets', 'Advanced', 'Language', 'Output Profile', and 'Report Calendar'. The main area displays a table of reports for 'Today (3)'.

| Report Name                                          | Format           | Time Range              | Devices      | Status  |
|------------------------------------------------------|------------------|-------------------------|--------------|---------|
| Security Analysis - app - HTTP-2020-11-24-1347_14808 | HTML PDF XML CSV | 2020/11/23 - 2020/11/23 | >124 Devices | 12s     |
| Security Analysis - app - SSH-2020-11-24-1346_14806  | HTML PDF XML CSV | 2020/11/23 - 2020/11/23 | >124 Devices | 11s     |
| Security Analysis - app - FTP-2020-11-24-1341_14804  | HTML PDF XML CSV | 2020/11/23 - 2020/11/23 | >124 Devices | 05m 25s |

## FortiDeceptor report

A new report template for FortiDeceptor has been added to FortiAnalyzer.

### To view the FortiDeceptor report template:

1. Go to *Reports > Report Definitions > Templates*.

*Template - FortiDeceptor Default Report* is available in the list of report templates, and you can click *HTML* or *PDF* in the *Preview* column to view a sample report.

You can create a new report using this template by clicking *Create New*.

The screenshot shows the 'Templates' section in FortiAnalyzer. The left sidebar is the same as the previous screenshot. The main area displays a table of report templates.

| Title                                              | Language | Description                                                                                                                                                                                                                                   | Category      | Preview     |
|----------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------|
| Template - FortiClient Vulnerability Scan Report   | English  | The vulnerabilities detected through Forticlient scans across the network                                                                                                                                                                     | FortiClient   | HTML<br>PDF |
| Template - FortiDDoS Default Report                | English  | Attacks and attackers by time period. Top 20 attacks, attack types, destinations and destinations by type.                                                                                                                                    | FortiDDoS     | HTML<br>PDF |
| Template - FortiDeceptor Default Report            | English  | Present a quick summary of incidents and alerts generated by FortiDeceptor                                                                                                                                                                    | FortiDeceptor | HTML<br>PDF |
| Template - FortiGate Performance Statistics Report | English  | FortiGate Performance Statistics Report.                                                                                                                                                                                                      | System        | HTML<br>PDF |
| Template - FortiMail Analysis Report               | English  | Statistics for Avg and Total mail size, number of mails and connections, delays, ip policies, recipient policies, top access list. Incoming filters for top spammed domains and users, classifiers by hour and disposition, and top subjects. | FortiMail     | HTML<br>PDF |
| Template - FortiMail Default Report                | English  | Top 10 client IP, senders, virus senders, local users, recipients and virus recipients                                                                                                                                                        | FortiMail     | HTML<br>PDF |
| Template - FortiNAC Endpoints and Network Report   | English  | FortiNAC Endpoints and Network Report.                                                                                                                                                                                                        | FortiNAC      | HTML<br>PDF |

The report template can be run or customized in the *All Reports* pane. A total of eight datasets and charts have been created to support the FortiDeceptor report, visible in *Chart Library* and *Datasets*.



| Reports            |                                                                                                                                                                                                                                                  |                                                          |               |                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|---------------|----------------------|
| Generated Reports  | <a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Clone</a> <a href="#">Export</a> <a href="#">Import</a> <input checked="" type="checkbox"/> Show Predefined <input checked="" type="checkbox"/> Show Custom |                                                          |               |                      |
| Report Definitions |                                                                                                                                                                                                                                                  |                                                          |               |                      |
| All Reports        |                                                                                                                                                                                                                                                  |                                                          |               |                      |
| Templates          |                                                                                                                                                                                                                                                  |                                                          |               |                      |
| Chart Library      |                                                                                                                                                                                                                                                  |                                                          |               |                      |
| Macro Library      |                                                                                                                                                                                                                                                  |                                                          |               |                      |
| Datasets           |                                                                                                                                                                                                                                                  |                                                          |               |                      |
| Advanced           |                                                                                                                                                                                                                                                  |                                                          |               |                      |
| Language           |                                                                                                                                                                                                                                                  |                                                          |               |                      |
| Output Profile     |                                                                                                                                                                                                                                                  |                                                          |               |                      |
| Report Calendar    |                                                                                                                                                                                                                                                  |                                                          |               |                      |
|                    | <input type="checkbox"/> Name                                                                                                                                                                                                                    | Description                                              | ▲ Device Type | Category             |
|                    | <input type="checkbox"/> FortiDDoS-Top 20 Attacks                                                                                                                                                                                                | Top 20 Attacks                                           | FortiDDoS     | Intrusion Prevention |
|                    | <input type="checkbox"/> FortiDDoS-Top 20 Destinations                                                                                                                                                                                           | Top 20 Destinations                                      | FortiDDoS     | Intrusion Prevention |
|                    | <input type="checkbox"/> FortiDDoS-Top 20 Destinations by Type                                                                                                                                                                                   | Top 20 Destinations by Type                              | FortiDDoS     | Intrusion Prevention |
|                    | <input checked="" type="checkbox"/> FortiDeceptor-FortiDeceptor-Top Attack Tools Based On IPS Alerts                                                                                                                                             | Top 10 Attack Tools Based On IPS Alerts                  | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> FortiDeceptor-FortiDeceptor-Top Attacker IPs Based On IPS Alerts                                                                                                                                             | Top 10 Attacker IPs Based on IPS Alerts                  | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> FortiDeceptor-FortiDeceptor-Top Attacker IPs By Incidents                                                                                                                                                    | Top 10 Attackers IPs by Incidents                        | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> FortiDeceptor-FortiDeceptor-Top Failed Login By Username                                                                                                                                                     | Top 10 Failed Login by Username                          | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> FortiDeceptor-FortiDeceptor-Top Malicious Files By Incidents                                                                                                                                                 | Top 10 Malicious Files by Incidents                      | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> FortiDeceptor-FortiDeceptor-Top Malicious URL Based On Web Filter Alerts                                                                                                                                     | Top 10 Malicious URL Access Based on Web Filter Alerts   | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> FortiDeceptor-FortiDeceptor-Top Services By Incidents                                                                                                                                                        | Top 10 Services by Incidents                             | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> FortiDeceptor-FortiDeceptor-Top Victim IPs By Incident                                                                                                                                                       | Top 10 Victim IPs by Incidents                           | FortiDeceptor | Event                |
|                    | <input type="checkbox"/> FortiFirewall-Active Traffic Users                                                                                                                                                                                      | List of active traffic users                             | FortiFirewall | Traffic              |
|                    | <input type="checkbox"/> FortiFirewall-Bandwidth Summary                                                                                                                                                                                         | Traffic bandwidth usage summary                          | FortiFirewall | Traffic              |
|                    | <input type="checkbox"/> FortiFirewall-Session Summary                                                                                                                                                                                           | Session summary                                          | FortiFirewall | Traffic              |
|                    | <input type="checkbox"/> FortiFirewall-Top 30 Applications by Bandwidth and Sessions                                                                                                                                                             | Top 30 applications by bandwidth usage and session count | FortiFirewall | Traffic              |
|                    | <input type="checkbox"/> FortiFirewall-Top 30 Destinations by Bandwidth and Sessions                                                                                                                                                             | Top 30 destinations by bandwidth usage and session count | FortiFirewall | Traffic              |

| Reports            |                                                                                                                                                             |               |                      |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|----------------------|
| Generated Reports  | <a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Clone</a> <a href="#">Validate</a> <a href="#">Validate All Custom</a> |               |                      |
| Report Definitions |                                                                                                                                                             |               |                      |
| All Reports        |                                                                                                                                                             |               |                      |
| Templates          |                                                                                                                                                             |               |                      |
| Chart Library      |                                                                                                                                                             |               |                      |
| Macro Library      |                                                                                                                                                             |               |                      |
| Datasets           |                                                                                                                                                             |               |                      |
| Advanced           |                                                                                                                                                             |               |                      |
| Language           |                                                                                                                                                             |               |                      |
| Output Profile     |                                                                                                                                                             |               |                      |
| Report Calendar    |                                                                                                                                                             |               |                      |
|                    | <input type="checkbox"/> Name                                                                                                                               | ▲ Device Type | Log Type             |
|                    | <input type="checkbox"/> fdd-Attacks-Timeline                                                                                                               | FortiDDoS     | Intrusion Prevention |
|                    | <input type="checkbox"/> fdd-Top-Attack-Types                                                                                                               | FortiDDoS     | Intrusion Prevention |
|                    | <input type="checkbox"/> fdd-Top-Attacks                                                                                                                    | FortiDDoS     | Intrusion Prevention |
|                    | <input type="checkbox"/> fdd-Top-Destinations                                                                                                               | FortiDDoS     | Intrusion Prevention |
|                    | <input type="checkbox"/> fdd-Top-Destinations-by-Type                                                                                                       | FortiDDoS     | Intrusion Prevention |
|                    | <input checked="" type="checkbox"/> fdc-Attack-Tool-Based-On-IPS-Alerts                                                                                     | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> fdc-Attacker-IPs-Based-On-IPS-Alerts                                                                                    | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> fdc-Failed-Login-By-User                                                                                                | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> fdc-Malicious-Files-By-Incident                                                                                         | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> fdc-Top-Attacker-IP-By-Incident                                                                                         | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> fdc-Top-Malicious-URL-Access-Based-On-Web-Filter-Alerts                                                                 | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> fdc-Top-Services-By-Incidents                                                                                           | FortiDeceptor | Event                |
|                    | <input checked="" type="checkbox"/> fdc-Top-Victim-IP-By-Incident                                                                                           | FortiDeceptor | Event                |
|                    | <input type="checkbox"/> ffw-Top-App-By-Bandwidth                                                                                                           | FortiFirewall | Traffic              |
|                    | <input type="checkbox"/> ffw-bandwidth-app-Top-Dest-By-Bandwidth-Sessions                                                                                   | FortiFirewall | Traffic              |
|                    | <input type="checkbox"/> ffw-bandwidth-app-Top-Users-By-Bandwidth                                                                                           | FortiFirewall | Traffic              |
|                    | <input type="checkbox"/> ffw-bandwidth-app-Traffic-By-Active-User-Number                                                                                    | FortiFirewall | Traffic              |

## Central UEBA table for custom reporting and widgets

This is an enhancement to the current UEBA feature which enables users to query central UEBA tables by running custom report.

**To create a report dataset based on the central UEBA table:**

1. On FortiAnalyzer, go to *Reports > Report Definitions > Datasets*.
2. Click *Create New* to create a new dataset based on \$ADOM\_UEBA\_USERS and \$ADOM\_UEBA\_HOSTS.

3. Click **Test** to view test results.

**Create Dataset**

**Dataset**

Name: test UEBA table

Log Type: Appevent

Query: select user\_group, host\_name, host\_ip, from itime(t1.lastseen) as last\_seen from \$ADOM UEBA\_USERS t1 join \$ADOM UEBA\_HOSTS t2 on t1.adomoid=t2.adomoid where nullifna(user\_group) is not null order by last\_seen desc

Variables

| Variable                       | Expression | Description |
|--------------------------------|------------|-------------|
| Click here to add a new entry. |            |             |

**Test query with specified devices and time period**

Time Period: Last 7 Days

Devices: ☒ All Devices ☐ Specify

**Test Result**

| user_group | host_name         | host_ip       | last_seen |
|------------|-------------------|---------------|-----------|
| FAC_Group  | T420-PC           | 172.17.241.23 | 2021-01-1 |
| FAC_Group  | 172.18.80.21      | 172.18.80.21  | 2021-01-1 |
| FAC_Group  | 172.18.27.183     | 172.18.27.183 | 2021-01-1 |
| FAC_Group  | PS421E3X16000437  | 172.17.59.42  | 2021-01-1 |
| FAC_Group  | 10.36.231.224     | 10.36.231.224 | 2021-01-1 |
| FAC_Group  | 10.59.34.60       | 10.59.34.60   | 2021-01-1 |
| FAC_Group  | 10.3.129.50       | 10.3.129.50   | 2021-01-1 |
| FAC_Group  | 172.18.245.1      | 172.18.245.1  | 2021-01-1 |
| FAC_Group  | Yuvinnings-iPhone | 172.17.248.22 | 2021-01-1 |
| FAC_Group  | 10.160.72.60      | 10.160.72.60  | 2021-01-1 |
| FAC_Group  | 172.19.28.59      | 172.19.28.59  | 2021-01-1 |

## 4. Run a report based on the dataset. The report is generated successfully and contains information from the UEBA central table.

UEBA Central Table test

| #  | Client(Group) | host_name            | host_ip        | last_seen           |
|----|---------------|----------------------|----------------|---------------------|
| 1  | FAC_Group     | VAN-201520-PC        | 172.16.67.130  | 2021-01-15 12:07:33 |
| 2  | FAC_Group     | 10.6.212.71          | 10.6.212.71    | 2021-01-15 12:07:33 |
| 3  | FAC_Group     | FortiFone FON-175    | 172.19.28.88   | 2021-01-15 12:07:33 |
| 4  | FAC_Group     | 172.16.179.39        | 172.16.179.39  | 2021-01-15 12:07:33 |
| 5  | FAC_Group     | VAN-801156-LT        | 172.17.248.20  | 2021-01-15 12:07:33 |
| 6  | FAC_Group     | CentOs7-Uefi         | 172.17.70.176  | 2021-01-15 12:07:33 |
| 7  | FAC_Group     | 172.16.196.252       | 172.16.196.252 | 2021-01-15 12:07:33 |
| 8  | FAC_Group     | 172.16.197.57        | 172.16.197.57  | 2021-01-15 12:07:33 |
| 9  | FAC_Group     | LAPTOP-E1Q5SL04      | 172.16.199.19  | 2021-01-15 12:07:33 |
| 10 | FAC_Group     | VAN-200599-FP        | 172.16.62.71   | 2021-01-15 12:07:33 |
| 11 | FAC_Group     | 172.18.78.163        | 172.18.78.163  | 2021-01-15 12:07:33 |
| 12 | FAC_Group     | 172.18.69.110        | 172.18.69.110  | 2021-01-15 12:07:33 |
| 13 | FAC_Group     | 172.17.74.136        | 172.17.74.136  | 2021-01-15 12:07:33 |
| 14 | FAC_Group     | FortiFone FON-175    | 172.19.28.89   | 2021-01-15 12:07:33 |
| 15 | FAC_Group     | 172.17.217.10        | 172.17.217.10  | 2021-01-15 12:07:33 |
| 16 | FAC_Group     | 172.18.74.159        | 172.18.74.159  | 2021-01-15 12:07:33 |
| 17 | FAC_Group     | 172.16.199.228       | 172.16.199.228 | 2021-01-15 12:07:33 |
| 18 | FAC_Group     | Martin-iPhone        | 172.17.240.21  | 2021-01-15 12:07:33 |
| 19 | FAC_Group     | VAN-201290-KRSHN     | 172.16.63.101  | 2021-01-15 12:07:33 |
| 20 | FAC_Group     | 172.16.97.25         | 172.16.97.25   | 2021-01-15 12:07:33 |
| 21 | FAC_Group     | 172.16.99.5          | 172.16.99.5    | 2021-01-15 12:07:33 |
| 22 | FAC_Group     | 172.17.61.173        | 172.17.61.173  | 2021-01-15 12:07:33 |
| 23 | FAC_Group     | VAN-201169-LT1       | 172.17.74.135  | 2021-01-15 12:07:33 |
| 24 | FAC_Group     | LG-Ericsson FON-460i | 172.16.98.206  | 2021-01-15 12:07:33 |
| 25 | FAC_Group     | 172.16.79.83         | 172.16.79.83   | 2021-01-15 12:07:33 |
| 26 | FAC_Group     | 172.30.144.210       | 172.30.144.210 | 2021-01-15 12:07:33 |
| 27 | FAC_Group     | 172.16.197.135       | 172.16.197.135 | 2021-01-15 12:07:33 |
| 28 | FAC_Group     | 172.16.94.39         | 172.16.94.39   | 2021-01-15 12:07:33 |
| 29 | FAC_Group     | romeo-pc2            | 169.254.83.9   | 2021-01-15 12:07:33 |
| 30 | FAC_Group     | 172.16.198.167       | 172.16.198.167 | 2021-01-15 12:07:33 |

## FortiSandbox CTAP report

A new FortiSandbox report covers file scan statistics with detected incidents, malware, and targeted hosts.

## To view the FortiSandbox CTAP report:

1. Go to Reports > Report Definitions > Templates.

*Template - FortiSandbox CTAP Report* is available in the list of report templates, and you can click *HTML* or *PDF* in the *Preview* column to view a sample report.

| Title                                               | Language | Description                                                                                                                                                                                                                                                                                                                                                                                                                                 | Category     | Preview             |
|-----------------------------------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------------------|
| Template - FortiPortal User Summary Report          | English  | FortiPortal User Summary Report.                                                                                                                                                                                                                                                                                                                                                                                                            | Fabric       | HTML<br>PDF         |
| Template - FortiProxy Default Report                | English  | Global bandwidth savings, cache rate, traffic and request timeline. Top 20 websites by bandwidth, bandwidth savings, cache rate, response time improvement.                                                                                                                                                                                                                                                                                 | FortiProxy   | HTML<br>PDF         |
| Template - FortiProxy Security Analysis             | English  | User Security Analysis                                                                                                                                                                                                                                                                                                                                                                                                                      | FortiProxy   | HTML<br>PDF         |
| Template - FortiProxy Web Usage Report              | English  | Web Usage Summary                                                                                                                                                                                                                                                                                                                                                                                                                           | FortiProxy   | HTML<br>PDF         |
| <b>Template - FortiSandbox CTAP Report</b>          | English  | FortiSandbox CTAP Report                                                                                                                                                                                                                                                                                                                                                                                                                    | FortiSandbox | <b>HTML<br/>PDF</b> |
| Template - FortiSandbox Default Report              | English  | Threat rating distribution, job severity timeline, malware severity of targeted hosts, top 20 targeted hosts, top 20 malware, top 50 file type and brief job list                                                                                                                                                                                                                                                                           | FortiSandbox | HTML<br>PDF         |
| Template - FortiWeb Default Report                  | English  | Top sources, sources of attacks, event categories, login events by user, top destinations, attack destinations and event types                                                                                                                                                                                                                                                                                                              | FortiWeb     | HTML<br>PDF         |
| Template - FortiWeb Web Application Analysis Report | English  | It includes web application trends, behavior and consolidated views in a multi-FortiWeb environment.                                                                                                                                                                                                                                                                                                                                        | FortiWeb     | HTML<br>PDF         |
| Template - Fortinet Email Risk Assessment           | English  | Email remains a critical tool for business, as well as a successful delivery vehicle for cybercriminals. To assess your organization's exposure, we added Fortinet's secure email gateway - FortiMail Cloud (including various advanced threat defense capabilities) in bcc mode in order to receive a copy of all email traffic being delivered by your current in-built security to both your end users' inboxes and external recipients. | Fabric       | HTML<br>PDF         |
| Template - GTP Report                               | English  | GTP Report.                                                                                                                                                                                                                                                                                                                                                                                                                                 | System       | HTML<br>PDF         |
| Template - High Bandwidth Application Usage Report  | English  | High Bandwidth Application Usage Report.                                                                                                                                                                                                                                                                                                                                                                                                    | Application  | HTML<br>PDF         |
| Template - Hourly Website Hits                      | English  | Hourly Website Hits                                                                                                                                                                                                                                                                                                                                                                                                                         | Web          | HTML<br>PDF         |
| Template - IPS Report                               | English  | Intrusions detected by type, severity, victims, sources, blocked, monitored, attacks over http-https.                                                                                                                                                                                                                                                                                                                                       | Security     | HTML<br>PDF         |
| Template - PCI-DSS Compliance Review                | English  | Summaries for PCI DSS Compliance and Regulatory Requirements, Related Best Security Practices, PCI DSS 3.1 Regulation Details.                                                                                                                                                                                                                                                                                                              | Security     | HTML<br>PDF         |
| Template - SOC Incident Report                      | English  | Present a brief summary of SOC Incidents.                                                                                                                                                                                                                                                                                                                                                                                                   | Security     | HTML<br>PDF         |

You can create a new report using this template by clicking *Create New*.

The report template can be run or customized in the *All Reports* pane.

| Title                                    | Language | Cache Status | Time Period | Devices       | Schedule | Report Owner |
|------------------------------------------|----------|--------------|-------------|---------------|----------|--------------|
| FortiGate Performance Statistics Report  | English  |              |             |               |          |              |
| FortiMail Analysis Report                | English  |              |             |               |          |              |
| FortiMail Default Report                 | English  |              |             |               |          |              |
| FortiNAC Endpoints and Network Report    | English  |              |             |               |          |              |
| Fortinet Email Risk Assessment           | English  |              |             |               |          |              |
| FortiPortal User Summary Report          | English  |              |             |               |          |              |
| FortiProxy Default Report                | English  |              |             |               |          |              |
| FortiProxy Security Analysis             | English  |              |             |               |          |              |
| FortiProxy Web Usage Report              | English  |              |             |               |          |              |
| <b>FortiSandbox CTAP Report</b>          | English  |              | This Week   | All_Device    |          | admin        |
| FortiSandbox Default Report              | English  |              |             |               |          |              |
| FortiWeb Default Report                  | English  |              |             |               |          |              |
| FortiWeb Web Application Analysis Report | English  |              |             |               |          |              |
| GTP Report                               | English  |              |             |               |          |              |
| High Bandwidth Application Usage Report  | English  |              | This Week   | All_Device    |          |              |
| IPS Report                               | English  |              |             |               |          |              |
| mysubnet                                 | English  |              | This Week   | All_Device    |          | admin        |
| PCI-DSS Compliance Review                | English  |              |             |               |          |              |
| SaaS Application Usage Report            | English  |              |             |               |          |              |
| Secure SD-WAN Assessment Report          | English  |              |             |               |          |              |
| Secure SD-WAN Report                     | English  |              | Last N Days | All_FortiGate |          |              |
| Security Analysis                        | English  |              |             |               |          |              |
| Security Events and Incidents Summary    | English  |              |             |               |          |              |
| Self-Harm and Risk Indicators Report     | English  |              |             |               |          |              |
| Situation Awareness Report               | English  |              |             |               |          |              |
| SOC Incident Report                      | English  |              | Last 7 Days | All_FortiGate |          |              |
| Social Media Usage Report                | English  |              |             |               |          |              |
| Threat Report                            | English  |              |             |               |          |              |

Below is a sample of the information included with the FortiSandbox CTAP Report.

| FortiSandbox CTAP Report                           |  |
|----------------------------------------------------|--|
| <b>Executive Summary</b>                           |  |
| Security                                           |  |
| File Analysis                                      |  |
| Performance                                        |  |
| <b>Security</b>                                    |  |
| Top 5 Known Malware Detected                       |  |
| Top 5 Unknown Malware Detected                     |  |
| Malware Disposition Breakdown                      |  |
| Top 5 Targeted Hosts                               |  |
| <b>File Analysis</b>                               |  |
| Total Files Scanned Clean to Malicious             |  |
| Filetype Breakout (Overall)                        |  |
| Filetype Breakout (Malware)                        |  |
| Compressed File Analysis (Malware)                 |  |
| <b>Performance</b>                                 |  |
| Files Scanned per Day and Hour                     |  |
| Top 10 Average Scan Time per Filetype (in seconds) |  |
| <b>Appendix A</b>                                  |  |
| Devices (7)                                        |  |

## FortiSandbox CTAP Report

Report Date: March 11, 2021 10:34

Data Range: 2020-08-23 00:00:00 2021-03-10 23:59:59PST (FAZ local)

### Executive Summary

The assessment report provides organizations a snapshot of their current security posture based on known and unknown malware found in the network. Through the use of sandboxing, organizations can better understand the benefits of using sandbox to uncover potential vulnerabilities in their security architecture and policies, and review the details of these threats.

#### Security



42

Known Malware Detected



45

Unknown Malware Detected

**Security Summary:** As part of your security strategy, protecting against known and unknown malware is critical to reducing risks. In-place security controls are designed to block known malware while sandboxing complements these controls to block unknown malware. Also critical is to uncover any callbacks as a signal to an active or impending threat campaign.

Additional details are found in Security section below.

#### File Analysis



400,211

Total Files Scanned



29

Unique Filetypes Found



136,513

Files Detected as Executable

Based on the number of files submitted for sandboxing, you will be provided intelligence on the various file types including those that are potentially risky found in your organization. This visibility serves as an opportunity for organizations to fine-tune application policies as part of early preventive controls.

Additional details are found in File Analysis section below.

#### Performance



8 s



318



617

## Organize reports in folders

Reports are organized in folders and sorted per data sources and the areas of interest for consistency and better usability.

For all upgraded and existing ADOMs, the reports layout structure and configuration will remain the same as before.

For newly created ADOMs, the reorganized folder structure feature is available. All reports, excluding the new Daily Summary Report, are sorted into folders by the report data sources and area of interest.

## To view report folders :

1. In an existing/upgraded ADOM, go to **Reports > Report Definitions > All Reports**.

For all upgraded and existing ADOMs, the reports layout structure and configuration will remain the same as before.

| Title                                   | Language | Cache Status | Time Period | Devices       | Schedule | Report Owner |
|-----------------------------------------|----------|--------------|-------------|---------------|----------|--------------|
| Application                             |          |              |             |               |          |              |
| Detailed User Report                    | English  |              |             |               |          |              |
| FortiClient Report                      | English  |              |             |               |          |              |
| Outbreak Alert Reports                  | English  |              |             |               |          |              |
| Web                                     | English  |              |             |               |          |              |
| 360 Protection Report                   | English  |              | Last 7 Days | All_Device    |          |              |
| 360-Degree Security Review              | English  |              |             |               |          |              |
| Admin and System Events Report          | English  |              |             |               |          |              |
| Application Risk and Control            | English  |              | Last 7 Days | All_FortiGate |          |              |
| Bandwidth and Applications Report       | English  |              |             |               |          |              |
| Client Reputation                       | English  |              |             |               |          |              |
| Cyber Threat Assessment                 | English  |              | Last 7 Days | All_FortiGate |          |              |
| Cyber-Bullying Indicators Report        | English  |              |             |               |          |              |
| Data Loss Prevention Detailed Report    | English  |              |             |               |          |              |
| Detailed Application Usage and Risk     | English  |              |             |               |          |              |
| DNS Report                              | English  |              |             |               |          |              |
| Email Report                            | English  |              |             |               |          |              |
| Endpoint Sandbox Detections Report      | English  |              |             |               |          |              |
| FortiCache Default Report               | English  |              |             |               |          |              |
| FortiCache Security Analysis            | English  |              |             |               |          |              |
| FortiCache Web Usage Report             | English  |              |             |               |          |              |
| FortiDox Default Report                 | English  |              | Last 7 Days | All_FortiDox  |          |              |
| FortiGate Performance Statistics Report | English  |              |             |               |          |              |

A new **Daily Summary Report** template is available in upgraded Fabric and FortiGate ADOMs. Administrators can create and customize daily summary reports using this template.

| Title                                           | Language       | Description                                                                                                                                                   | Category        | Preview         |
|-------------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-----------------|
| Template - 360 Protection Report                | English        | Present a brief summary of hardware/software inventory of the FortiGate devices over a 30 day period.                                                         | System          | HTML PDF        |
| Template - 360-Degree Security Review           | English        | Security review of Application Visibility and Control, Threat Detection, Data Exfiltration Detection, Endpoint Detection, Prevention and Recommended Actions. | Security        | HTML PDF        |
| Template - Admin and System Events Report       | English        | Admin login and failed login attempts and system severity event counts.                                                                                       | System          | HTML PDF        |
| Template - Application Risk and Control         | English        | Application risk, categories, bandwidth by app, web categories, vulnerability exploits, virus, botnet, adware malicious attacks, file transfers.              | Application     | HTML PDF        |
| Template - Bandwidth and Applications Report    | English        | Traffic, Bandwidth, Sessions, Destinations summaries - by users and applications                                                                              | Application     | HTML PDF        |
| Template - Client Reputation                    | English        | Client and user network behaviour, incidents by user, devices, threat summary.                                                                                | User            | HTML PDF        |
| Template - Cyber Threat Assessment              | English        | Cyber Threat review of Application Visibility and Control, Threat Detection, Prevention and Recommended Actions.                                              | Security        | HTML PDF        |
| Template - Cyber-Bullying Indicators Report     | English        | Cyber-Bullying Indicators Report.                                                                                                                             | Application     | HTML PDF        |
| Template - DNS Report                           | English        | Summarizes the suspicious or high risk DNS activity on the network.                                                                                           | System          | HTML PDF        |
| <b>Template - Daily Summary Report</b>          | <b>English</b> | <b>Present a brief summary report about traffic, threat, app, user, incident, compromised host and so on.</b>                                                 | <b>Security</b> | <b>HTML PDF</b> |
| Template - Data Loss Prevention Detailed Report | English        | Violation Summary and Activity Details of Email, Web, and FTP.                                                                                                | Security        | HTML PDF        |
| Template - Detailed Application Usage and Risk  | English        | Application Risk - botnet, proxy avoidance, peer-to-peer, remote access, email, Backup and storage, general access. Includes risk category examples.          | Application     | HTML PDF        |
| Template - Email Report                         | English        | Email Senders and Recipients by Total Number and Size of emails.                                                                                              | Security        | HTML PDF        |
| Template - Endpoint Sandbox Detections Report   | English        | Endpoint report showing the APT threats detected by sandbox                                                                                                   | FortiSandbox    | HTML PDF        |

2. In a Fabric ADOM created in FortiAnalyzer 7.0.0, go to **Reports > Report Definitions > All Reports**.

For newly created ADOMs, the reorganized folder structure feature is available. All reports, excluding the new Daily Summary Report, are sorted into folders by the report data sources and area of interest.

| Run Report | Report | Folder | More | Show Scheduled Only | Title                  | Language | Cache Status | Time Period | Devices       | Schedule         | Report Owner |
|------------|--------|--------|------|---------------------|------------------------|----------|--------------|-------------|---------------|------------------|--------------|
|            |        |        |      |                     | Application Reports    |          |              |             |               |                  |              |
|            |        |        |      |                     | Asset and User Reports |          |              |             |               |                  |              |
|            |        |        |      |                     | Compliance Reports     |          |              |             |               |                  |              |
|            |        |        |      |                     | Fabric Reports         |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiCache Reports     |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiClient Reports    |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiDDoS Reports      |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiDeceptor Reports  |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiFirewall Reports  |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiGate Reports      |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiMail Reports      |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiNAC Reports       |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiProxy Reports     |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiSandbox Reports   |          |              |             |               |                  |              |
|            |        |        |      |                     | FortiWeb Reports       |          |              |             |               |                  |              |
|            |        |        |      |                     | Network Reports        |          |              |             |               |                  |              |
|            |        |        |      |                     | Outbreak Alert Reports |          |              |             |               |                  |              |
|            |        |        |      |                     | SOC Reports            |          |              |             |               |                  |              |
|            |        |        |      |                     | Daily Summary Report   | English  | 0            | Yesterday   | All_FortiGate | Daily @ 03:00 AM |              |

Expand a data source folder to view reports within that folder that have the same data source assigned to it, for example *FortiGate Reports*.

| Run Report | Report | Folder | More | Show Scheduled Only | Title                                                | Language | Cache Status | Time Period | Devices       | Schedule | Report Owner |
|------------|--------|--------|------|---------------------|------------------------------------------------------|----------|--------------|-------------|---------------|----------|--------------|
|            |        |        |      |                     | Application Reports                                  |          |              |             |               |          |              |
|            |        |        |      |                     | Asset and User Reports                               |          |              |             |               |          |              |
|            |        |        |      |                     | Compliance Reports                                   |          |              |             |               |          |              |
|            |        |        |      |                     | Fabric Reports                                       |          |              |             |               |          |              |
|            |        |        |      |                     | FortiCache Reports                                   |          |              |             |               |          |              |
|            |        |        |      |                     | FortiClient Reports                                  |          |              |             |               |          |              |
|            |        |        |      |                     | FortiDDoS Reports                                    |          |              |             |               |          |              |
|            |        |        |      |                     | FortiDeceptor Reports                                |          |              |             |               |          |              |
|            |        |        |      |                     | FortiFirewall Reports                                |          |              |             |               |          |              |
|            |        |        |      |                     | FortiGate Reports                                    |          |              |             |               |          |              |
|            |        |        |      |                     | 360 Protection Report                                | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | 360-Degree Security Review                           | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Admin and System Events Report                       | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Application Risk and Control                         | English  |              | Last 7 Days | All_FortiGate |          |              |
|            |        |        |      |                     | Bandwidth and Applications Report                    | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Client Reputation                                    | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Cyber Threat Assessment                              | English  |              | Last 7 Days | All_FortiGate |          |              |
|            |        |        |      |                     | Cyber-Bullying Indicators Report                     | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Data Loss Prevention Detailed Report                 | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Detailed Application Usage and Risk                  | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | DNS Report                                           | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Email Report                                         | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | FortiClient Default Report from FortiGate            | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | FortiClient Vulnerability Scan Report from FortiGate | English  |              | Last 7 Days | All_Device    |          |              |

Expand an area of interest folder to view reports within that folder that belong to the same area of interest, for example *Application Reports*.

| Run Report | Report | Folder | More | Show Scheduled Only | Title                                          | Language | Cache Status | Time Period | Devices       | Schedule | Report Owner |
|------------|--------|--------|------|---------------------|------------------------------------------------|----------|--------------|-------------|---------------|----------|--------------|
|            |        |        |      |                     | Application Reports                            |          |              |             |               |          |              |
|            |        |        |      |                     | Application Risk and Control                   | English  |              | Last 7 Days | All_FortiGate |          |              |
|            |        |        |      |                     | Bandwidth and Applications Report              | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Detailed Application Usage and Risk            | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Email Report                                   | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | FortiCache Web Usage Report                    | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Fortinet Email Risk Assessment                 | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | FortiProxy Web Usage Report                    | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | FortiWeb Web Application Analysis Report       | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | GTP Report                                     | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | High Bandwidth Application Usage Report        | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Hourly Website Hits                            | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | SaaS Application Usage Report                  | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Secure SD-WAN Report                           | English  |              | Last 7 Days | All_FortiGate |          |              |
|            |        |        |      |                     | Top 20 Categories and Applications (Bandwidth) | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Top 20 Categories and Applications (Session)   | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Top 20 Category and Websites (Bandwidth)       | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Top 20 Category and Websites (Session)         | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Top 500 Sessions by Bandwidth                  | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | Top Allowed and Blocked with Timestamps        | English  |              | Last 7 Days | All_Device    |          |              |
|            |        |        |      |                     | User Detailed Browsing Log                     | English  |              | Last 7 Days | All_FortiGate |          |              |
|            |        |        |      |                     | User Top 500 Websites by Bandwidth             | English  |              | Last 7 Days | All_FortiGate |          |              |
|            |        |        |      |                     | Asset and User Reports                         |          |              |             |               |          |              |
|            |        |        |      |                     | Compliance Reports                             |          |              |             |               |          |              |
|            |        |        |      |                     | Fabric Reports                                 |          |              |             |               |          |              |
|            |        |        |      |                     | FortiCache Reports                             |          |              |             |               |          |              |
|            |        |        |      |                     | FortiClient Reports                            |          |              |             |               |          |              |

Reports that have mixed data sources are included in the *Fabric Reports* folder.

- In a FortiGate ADOM created in FortiAnalyzer 7.0.0, go to **Reports > Report Definitions > All Reports**. Reports available in the FortiGate ADOM are displayed with the new folder structure.

| Title                | Language | Cache Status | Time Period | Devices       | Schedule         | Report Owner |
|----------------------|----------|--------------|-------------|---------------|------------------|--------------|
| Daily Summary Report | English  | Yesterday    |             | All_FortiGate | Daily @ 03:00 AM |              |

- In a FortiSandbox ADOM created in FortiAnalyzer 7.0.0, go to **Reports > Report Definitions > All Reports**. Reports available in the FortiSandbox ADOM are displayed with the new folder structure.

| Title                              | Language | Cache Status | Time Period | Devices    | Schedule | Report Owner |
|------------------------------------|----------|--------------|-------------|------------|----------|--------------|
| Asset and User Reports             |          |              |             |            |          |              |
| Endpoint Sandbox Detections Report | English  |              | Last 7 Days | All_Device |          |              |
| FortiSandbox CTAP Report           | English  |              | Last 7 Days | All_Device |          |              |
| FortiSandbox Default Report        | English  |              | Last 7 Days | All_Device |          |              |
| FortiSandbox CTAP Report           | English  |              | Last 7 Days | All_Device |          |              |

## Additional charts for SD-WAN reporting - 7.0.1

The Secure SD-WAN Report now includes charts for SD-WAN Link Health Status and the Inbound/Outbound status per SD-WAN device interfaces.

### To view additional charts in the SD-WAN Report:

- Go to **Reports > Templates**.
- In the templates pane, right-click **Secure SD-WAN Report**, and click **Create Report**.

| Title                                                     | Language | Description                                                                                                                                                                                                                                                                                          | Category    | Preview  |
|-----------------------------------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------|
| Template - SOC Incident Report                            | English  | Present a brief summary of SOC Incidents.                                                                                                                                                                                                                                                            | Security    | HTML PDF |
| Template - SaaS Application Usage Report                  | English  | Summarizes the usage of SaaS apps compared to all applications, Sanctioned vs Unscheduled SaaS applications, and total bandwidth by SaaS Sanctioned and Unscheduled apps.                                                                                                                            | Application | HTML PDF |
| Template - Secure SD-WAN Assessment Report                | English  | Secure SD-WAN Assessment Report.                                                                                                                                                                                                                                                                     | System      | HTML PDF |
| Template - Secure SD-WAN Report                           | English  | Secure SD-WAN Report.                                                                                                                                                                                                                                                                                | System      | HTML PDF |
| Template - Security Analysis                              | English  | Security Analysis of traffic, application, user, destination, bandwidth and sessions. DHCP, Wifi, traffic history. Web usage by users, categories and sites. Top email by senders, recipients. Malware, botnet, intrusion detections, victims and sources. VPN usage. Admin Login and system events. | Security    | HTML PDF |
| Template - Security Events and Incidents Summary          | English  | Present a brief summary of the events/incidents collected.                                                                                                                                                                                                                                           | Security    | HTML PDF |
| Template - Self-Harm and Risk Indicators Report           | English  | Self-Harm and Risk Indicators Report.                                                                                                                                                                                                                                                                | Application | HTML PDF |
| Template - Situation Awareness Report                     | English  | Provide awareness of your current security posture, and allow for a better understanding of the 'big picture' which will help anticipate what may happen to networks and systems enabling the security team to provide corrective measures avoiding costly breaches or mishaps.                      | Security    | HTML PDF |
| Template - Social Media Usage Report                      | English  | Social Media Usage Report.                                                                                                                                                                                                                                                                           | Application | HTML PDF |
| Template - Threat Report                                  | English  | Malware, Botnets - detected, victims and sources. Intrusions detected, sources, blocked severity and timeline.                                                                                                                                                                                       | Security    | HTML PDF |
| Template - Throughput Utilization Billing Report          | English  | Interface Throughput Utilization Billing Report.                                                                                                                                                                                                                                                     | System      | HTML PDF |
| Template - Top 20 Categories and Applications (Bandwidth) | English  | Top 20 Categories and Applications (Bandwidth)                                                                                                                                                                                                                                                       | Application | HTML PDF |
| Template - Top 20 Categories and Applications (Session)   | English  | Top 20 Categories and Applications (Session)                                                                                                                                                                                                                                                         | Application | HTML PDF |

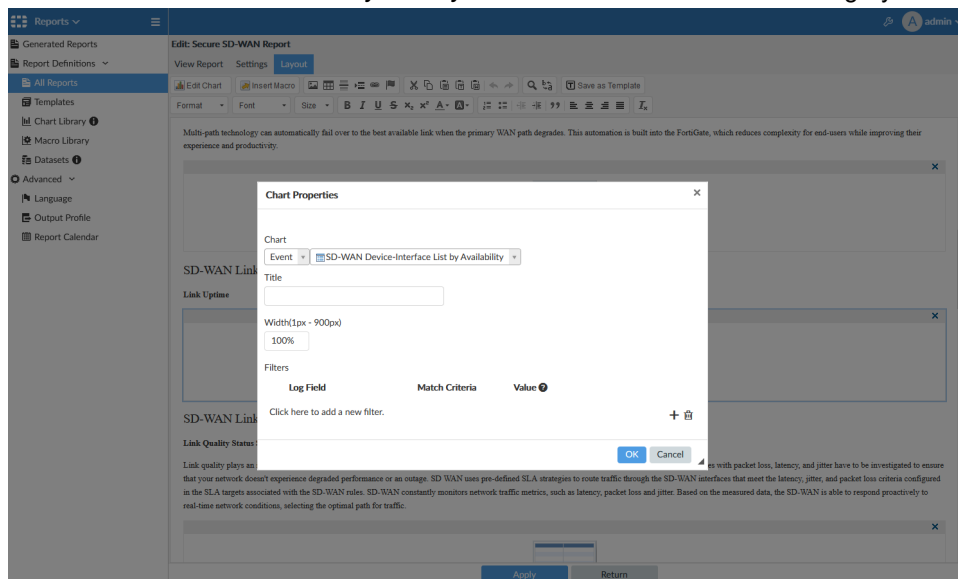
- In the tree menu, click **Report Definitions > All Reports**.

4. In the reports pane, expand *FortiGate Reports* and click *Secure SD-WAN Report*.

The screenshot shows the FortiAnalyzer Reports interface. On the left, the 'Reports' menu is expanded, showing 'Generated Reports' and 'Report Definitions'. Under 'Report Definitions', 'All Reports' is selected. The main pane displays a list of reports. The 'Secure SD-WAN Report' is highlighted in blue.

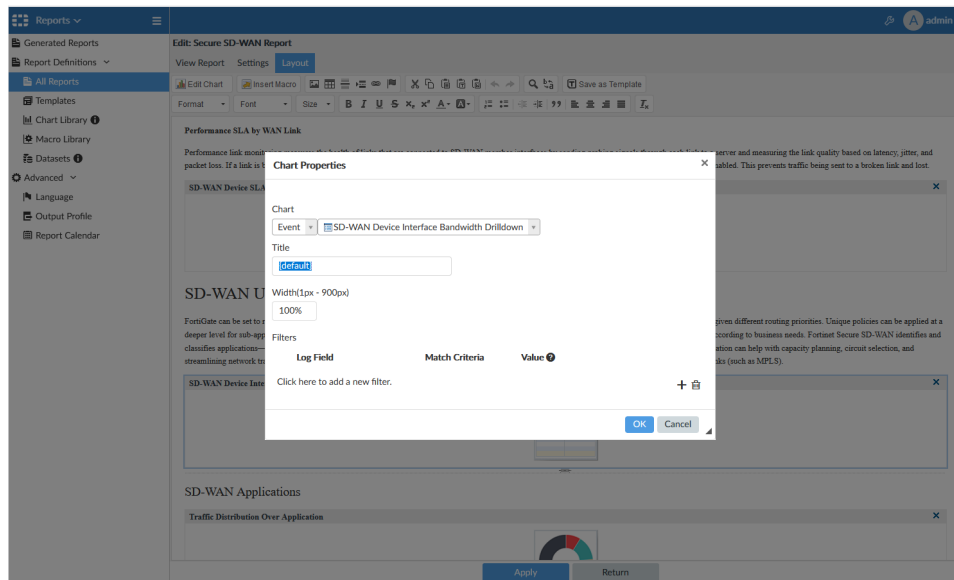
| Title                                                | Language | Cache Status | Time Period | Devices       | Schedule | Report Owner |
|------------------------------------------------------|----------|--------------|-------------|---------------|----------|--------------|
| FortiDeceptor Reports                                |          |              |             |               |          |              |
| FortiFirewall Reports                                |          |              |             |               |          |              |
| FortiGate Reports                                    |          |              |             |               |          |              |
| 360 Protection Report                                | English  |              | Last 7 Days | All_Device    |          |              |
| 360-Degree Security Review                           | English  |              | Last 7 Days | All_Device    |          |              |
| Admin and System Events Report                       | English  |              | Last 7 Days | All_Device    |          |              |
| Application Risk and Control                         | English  |              | Last 7 Days | All_FortiGate |          |              |
| Bandwidth and Applications Report                    | English  |              | Last 7 Days | All_Device    |          |              |
| Client Reputation                                    | English  |              | Last 7 Days | All_Device    |          |              |
| Cyber Threat Assessment                              | English  |              | Last 7 Days | All_FortiGate |          |              |
| Cyber-Bullying Indicators Report                     | English  |              | Last 7 Days | All_Device    |          |              |
| Data Loss Prevention Detailed Report                 | English  |              | Last 7 Days | All_Device    |          |              |
| Detailed Application Usage and Risk                  | English  |              | Last 7 Days | All_Device    |          |              |
| DNS Report                                           | English  |              | Last 7 Days | All_Device    |          |              |
| Email Report                                         | English  |              | Last 7 Days | All_Device    |          |              |
| FortiClient Default Report from FortiGate            | English  |              | Last 7 Days | All_Device    |          |              |
| FortiClient Vulnerability Scan Report from FortiGate | English  |              | Last 7 Days | All_Device    |          |              |
| FortiGate Performance Statistics Report              | English  |              | Last 7 Days | All_Device    |          |              |
| GTP Report                                           | English  |              | Last 7 Days | All_Device    |          |              |
| High Bandwidth Application Usage Report              | English  |              | Last 7 Days | All_Device    |          |              |
| Hourly Website Hits                                  | English  |              | Last 7 Days | All_Device    |          |              |
| IPS Report                                           | English  |              | Last 7 Days | All_Device    |          |              |
| PCI-DSS Compliance Review                            | English  |              | Last 7 Days | All_Device    |          |              |
| SaaS Application Usage Report                        | English  |              | Last 7 Days | All_Device    |          |              |
| Secure SD-WAN Assessment Report                      | English  |              | Last 7 Days | All_Device    |          |              |
| <b>Secure SD-WAN Report</b>                          | English  |              | Last 7 Days | All_FortiGate |          |              |
| Security Analysis                                    | English  |              | Last 7 Days | All_Device    |          |              |
| Security Events and Incidents Summary                | English  |              | Last 7 Days | All_Device    |          |              |

5. Click the *Layout* tab and scroll down to the *SD-WAN Link Health Status* chart, then click the *Chart Properties*. The *SD-WAN Device-Interface List by Activity* chart was added to the *Event* category.

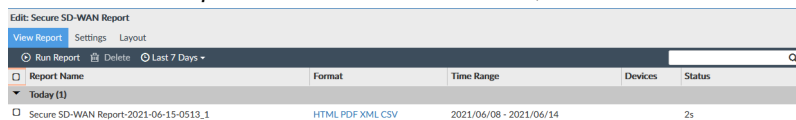


6. Scroll down to the *SD-WAN Utilization* section and click the *Chart Properties*. The *SD-WAN Device Interface Bandwidth Drilldown* chart was added to the *Event* category.





7. Click the **View Report** tab. In the **Format** column, click **PDF**.



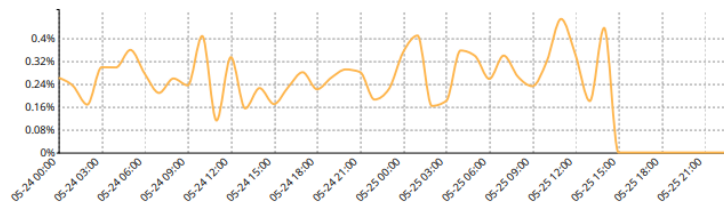
The Table of Contents displays the *SD-WAN Link Health Status* report.

## Table of Contents

|                                                              |    |
|--------------------------------------------------------------|----|
| Introduction Secure SD-WAN .....                             | 3  |
| SD-WAN Performance .....                                     | 4  |
| Overview of Device - FW61E-V64 .....                         | 4  |
| SD-WAN Availability .....                                    | 4  |
| Latency After SD-WAN Implementation (ms) .....               | 4  |
| Jitter After SD-WAN Implementation (ms) .....                | 5  |
| Packet Loss After SD-WAN Implementation .....                | 5  |
| Overview of Device - FG61F-V70 .....                         | 5  |
| SD-WAN Availability .....                                    | 5  |
| Latency After SD-WAN Implementation (ms) .....               | 6  |
| Jitter After SD-WAN Implementation (ms) .....                | 6  |
| Packet Loss After SD-WAN Implementation .....                | 7  |
| SD-WAN Link Health Status .....                              | 7  |
| SD-WAN Link Quality .....                                    | 10 |
| Device - FW61E-V64 .....                                     | 10 |
| Latency by WAN Link Over Time (ms) .....                     | 10 |
| Jitter by WAN Link Over Time (ms) .....                      | 11 |
| Packet Loss by WAN Link Over Time .....                      | 11 |
| Device - FG61F-V70 .....                                     | 11 |
| Latency by WAN Link Over Time (ms) .....                     | 11 |
| Jitter by WAN Link Over Time (ms) .....                      | 11 |
| Packet Loss by WAN Link Over Time .....                      | 12 |
| Service Level Agreements (SLAs) .....                        | 13 |
| Device - FW61E-V64 .....                                     | 13 |
| SLA Rules Link Percentage Within Latency Threshold .....     | 13 |
| SLA Rules Link Percentage Within Jitter Threshold .....      | 13 |
| SLA Rules Link Percentage Within Packet Loss Threshold ..... | 14 |
| Latency by SLA Rule Over Time (ms) .....                     | 14 |
| Jitter by SLA Rule Over Time (ms) .....                      | 14 |
| Packet Loss by SLA Rule Over Time .....                      | 15 |
| Device - FG61F-V70 .....                                     | 15 |
| SLA Rules Link Percentage Within Latency Threshold .....     | 15 |
| SLA Rules Link Percentage Within Jitter Threshold .....      | 16 |
| SLA Rules Link Percentage Within Packet Loss Threshold ..... | 17 |
| Latency by SLA Rule Over Time (ms) .....                     | 18 |
| Jitter by SLA Rule Over Time (ms) .....                      | 18 |
| Packet Loss by SLA Rule Over Time .....                      | 18 |
| SD-WAN Utilization .....                                     | 18 |
| Device - FW61E-V64 .....                                     | 18 |
| Traffic Utilization by SD-WAN Rule .....                     | 19 |
| Traffic Distribution Over SD-WAN Member .....                | 19 |
| Traffic Utilization by SD-WAN Members Over Time .....        | 19 |
| Sent(bps) .....                                              | 19 |
| Received(bps) .....                                          | 19 |

The *SD-WAN Device-Interface List by Availability* drilldown charts are displayed.

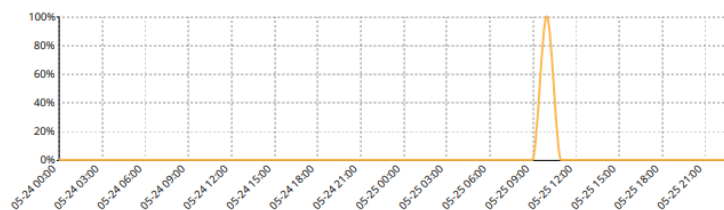
Packet Loss After SD-WAN Implementation



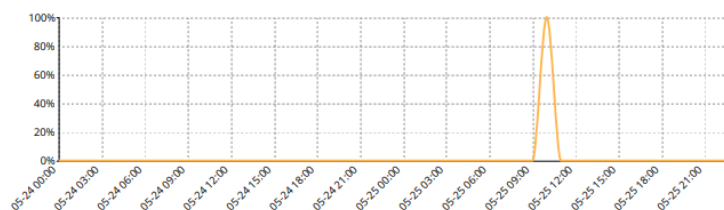
SD-WAN Link Health Status

**Link Uptime**

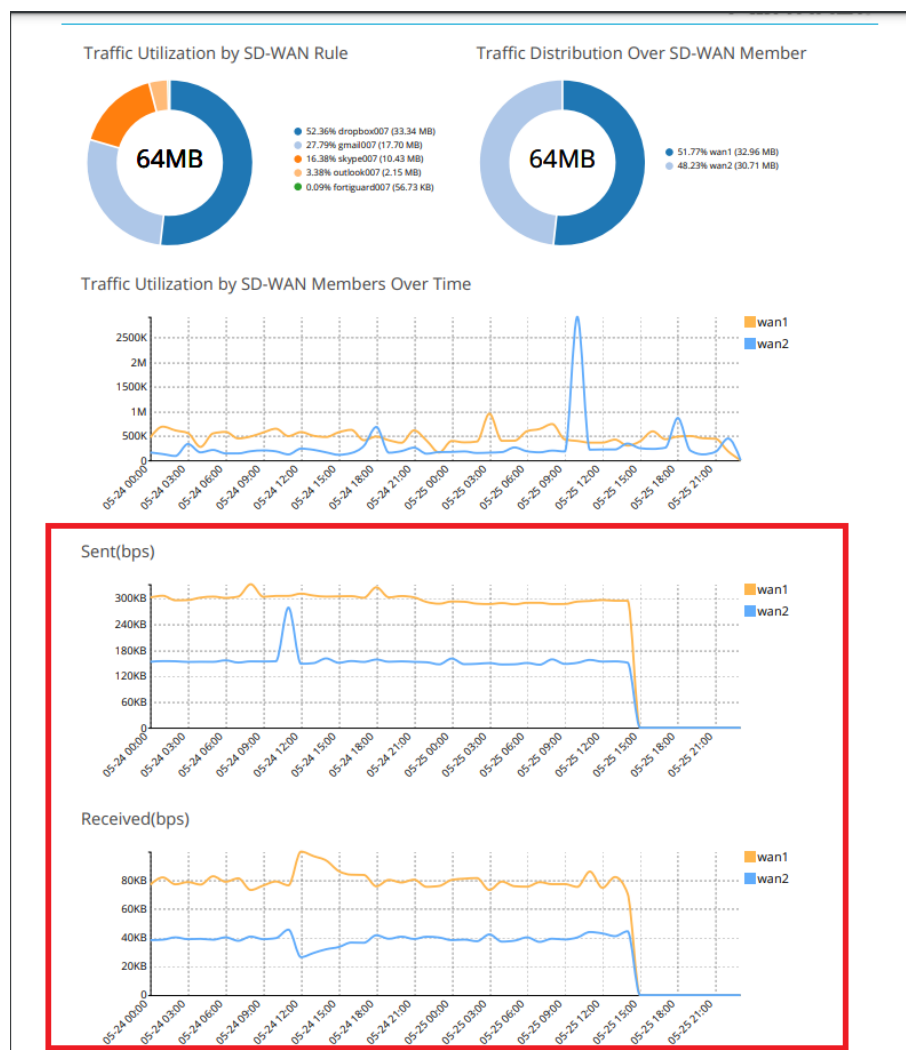
FGT61F-V70:VLAN1



FGT61F-V70:VLAN2



The *SD-Wan Device Interface Bandwidth Drilldown* charts are also displayed.



# System

This section lists the new features added to FortiAnalyzer for system settings:

- [Administrators on page 83](#)
- [ADOM on page 91](#)

## High Availability (HA)

This section lists the new features added to FortiAnalyzer for high availability (HA):

- [FortiAnalyzer HA graceful upgrade on page 81](#)

### FortiAnalyzer HA graceful upgrade

With this new feature, FortiAnalyzer HA supports graceful upgrading to avoid log loss, and also allow a trial period of the new image and support roll-back to the existing firmware if the new image has any issues.

In the following example, FortiAnalyzer HA is being upgraded from version 6.4.5 to 7.0.0, and contains two members: *FAZ-1* is the Primary and *FAZ-2* is the Secondary.



Graceful upgrade is only supported when upgrading from 6.4.5 and above to version 7.0.0 and later.

Data conversion depends on each application using this framework to do the conversion between the different versions. In 7.0.0, only incident conversion is supported when syncing from a higher level version to lower level version.

---

#### To update FortiAnalyzer HA gracefully:

1. Upgrade FAZ-2, the Secondary unit, to the new version. In this example, FAZ-2 is upgraded from version 6.4.5 to 7.0.0.
2. After FAZ-2 is up and running, check that there are no critical crashes and that the Primary can still forward logs to the Secondary. Event Alert and Incidents still can be received from 6.4.5 to 7.0.0.
  - To check that there are no critical crashes, use the following CLI command:  
`diagnose debug crash read`
  - To check that logs are being forwarded, use the following CLI command:  
`diagnose test application logfwd 4`
  - To create an example to check event alert synchronization, log in to FortiAnalyzer using the wrong password to generate a new local event log, and check on both FAZ-1 and FAZ-2 to confirm that the event alert can be found on both devices.

FortiSoC

Dashboards

Playbooks

Incidents

Events

Outbreak Alerts

Automation

Connectors

Playbook

Playbook Monitor

Event Monitor

All Events

By Endpoint

By Threat

System Events

Handlers

Event Handler List

FortiGate Event Handlers

Subnet List

Incidents

HA PrimaryADOM: root

RefreshCustom View

All DevicesAllExpand AllShow Acknowledged

Handler = "Local Device Event"Add Filter

|                          | # | Event              | Event Status | Event Type | Coun | Severity | First Occurrence | Last Update    | Additional Info      | Handler            | Tags                                | Device Name      |
|--------------------------|---|--------------------|--------------|------------|------|----------|------------------|----------------|----------------------|--------------------|-------------------------------------|------------------|
| <input type="checkbox"/> | 1 | > User login/lo... |              | Event      | 1    | Medium   | 22 minutes ago   | 22 minutes ago | User 'rtrtr' logi... | Local Device Ev... | <input type="text" value="System"/> | FL-1KE3R16000419 |
| <input type="checkbox"/> | 2 | > Device offlin... |              | Event      | 16   | Medium   | 2 hours ago      | 2 hours ago    | Did not receive...   | Local Device Ev... | <input type="text" value="System"/> | FL-1KE3R16000419 |

- To create an example to check incident synchronization, create a new incident on FAZ-1, then check on FAZ-2 to see if it was correctly synced across devices.

| #  | Incident Number | Incident Date / Time | Incident Reporter              | Incident Category   | Severity | Status   | Affected Endpoint | Description               |
|----|-----------------|----------------------|--------------------------------|---------------------|----------|----------|-------------------|---------------------------|
| 1  | IN00039969      | 2021-06-16 14:52:59  | admin                          | Unauthorized Access | Medium   | New      | N/A               | Test for HA upgrade sy... |
| 2  | IN00039968      | 2021-05-19 15:11:28  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | VAN-912483-PC1    | Intrusion detected.       |
| 3  | IN00039967      | 2021-05-19 15:10:58  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.193.15     | Intrusion detected.       |
| 4  | IN00039966      | 2021-05-19 15:10:26  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | DESKTOP-3Q19QFC   | Intrusion detected.       |
| 5  | IN00039965      | 2021-05-19 15:09:56  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | DESKTOP-3Q19QFC   | Intrusion detected.       |
| 6  | IN00039964      | 2021-05-19 15:03:44  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.193.11     | Intrusion detected.       |
| 7  | IN00039963      | 2021-05-19 15:02:40  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | jack              | Intrusion detected.       |
| 8  | IN00039962      | 2021-05-19 15:01:08  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | VAN-200150-PC10   | Intrusion detected.       |
| 9  | IN00039960      | 2021-05-19 15:01:08  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | VAN-200150-PC10   | Intrusion detected.       |
| 10 | IN00039961      | 2021-05-19 15:01:08  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | VAN-200150-PC10   | Intrusion detected.       |
| 11 | IN00039959      | 2021-05-19 15:00:06  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | VAN-200150-PC10   | Intrusion detected.       |
| 12 | IN00039958      | 2021-05-19 15:00:06  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | VAN-200150-PC10   | Intrusion detected.       |
| 13 | IN00039957      | 2021-05-19 15:00:06  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.193.8      | Intrusion detected.       |
| 14 | IN00039956      | 2021-05-19 14:57:00  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.193.8      | Intrusion detected.       |
| 15 | IN00039955      | 2021-05-19 14:47:39  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.193.8      | Intrusion detected.       |
| 16 | IN00039954      | 2021-05-19 14:44:01  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.31.70      | Intrusion detected.       |
| 17 | IN00039953      | 2021-05-19 14:41:57  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.31.160     | Intrusion detected.       |
| 18 | IN00039952      | 2021-05-19 14:41:27  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.31.160     | Intrusion detected.       |
| 19 | IN00039951      | 2021-05-19 14:36:16  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | van-905645-pc1    | Intrusion detected.       |
| 20 | IN00039950      | 2021-05-19 14:35:45  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | van-905645-pc1    | Intrusion detected.       |
| 21 | IN00039949      | 2021-05-19 14:22:48  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.30.118     | Intrusion detected.       |
| 22 | IN00039948      | 2021-05-19 14:22:16  | My Critical Intrusion Incident | Malicious Code      | High     | Analysis | 172.16.30.118     | Intrusion detected.       |

- Since both devices are now running on different firmware versions, configuration synchronization is unavailable at this time. You can check this setting using the `diagnose ha status` command in the FortiAnalyzer CLI. In this example, the config sync status is down, and no configuration changes can be synced from the Primary to Secondary unit.

```
diagnose ha status
HA-Status: Primary
up-time: 11h38m12.811s
config-sync: Allow
serial-no: FL-1KE3R16000432
fazuid: 2626920937
hostname: FAZ1000E-2
HA-Secondary HA1000e@192.168.1.90 FL-1KE3R16000419
ip: 192.168.1.90
```

```

serial-no: FL-1KE3R16000119
fazuid: 1239922567
hostname: FAZ1000E
conn-st: up
up/down-time: 11h38m10.455s
conn-msg: firmware version mismatch (v6.4.6-build2363 210531 (GA))
cfgsync-st: down
data-init-sync-st: done, 11h37m49.396s

```

4. Once FAZ-2 is in data-sync with FAZ-1, an administrator can trigger HA-failover using the CLI to switch FAZ-2 to the Primary role.

- a. In the FortiAnalyzer CLI, enter the command `diagnose ha failover` to make FAZ-2 the Primary.

```
FAZ1000E-1 # diagnose ha failover
```

- b. Use the command *diagnose ha status* to confirm the role of FAZ-2 as the new Primary.

```

FAZ1000E-2 # diagnose ha status
HA-Status: Primary
up-time: 11h38m12.811s
config-sync: Allow
serial-no: FL-1KE3R16000432
fazuid: 2626920937
hostname: FAZ1000E-2
HA-Secondary HA1000e@192.168.1.90 FL-1KE3R16000419
ip: 192.168.1.90
serial-no: FL-1KE3R16000119
fazuid: 1239922567
hostname: FAZ1000E
conn-st: up
up/down-time: 11h38m10.455s
conn-msg: firmware version mismatch (v6.4.6-build2363 210531 (GA))
cfgsync-st: down
data-init-sync-st: done, 11h37m49.396s

```

5. Now is the time for the administrator to try out the new image on FAZ-2.  
As part of the graceful upgrade, logs can still be forwarded from a higher version (7.0.0) to a lower version (6.4.5) without issue, and incidents are synched from the higher version (7.0.0) to the Secondary running a lower version (6.4.5).  
During this time you should avoid any configuration changes, as they will not be synchronized between versions.
6. Check the upgrade guide checklist to confirm the new Primary is working as expected.  
After a few hours or a day, FAZ-1 can be upgraded to the new firmware version (7.0.0). After FAZ-1 is upgraded, FAZ-2 will continue to operate as the Primary. You can failover again to return FAZ-1 to operating as the Primary, or keep FAZ-2 as the new Primary.

## Administrators

This section lists the new features added to FortiAnalyzer for administrators:

- [Theme mode on page 84](#)
- [Add operation permissions to Admin profile on page 85](#)
- [Admins can use a SAML SSO FortiCloud account to log in to FortiAnalyzer on page 89](#)

## Theme mode

When you create a new user, you can to apply a theme to all the administrator accounts, or allow admins to choose their own theme

### To enable themes per admin:

1. Go to *Admin > Administrators*.
2. In the toolbar, click *Create New*. The *New Administrator* page is displayed.

**New Administrator**

User Name: Admin

Avatar: + Change Photo - Remove Photo

Comments:

Admin Type: LOCAL

New Password:

Confirm Password:

Admin Profile: Restricted\_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify

JSON API Access: None

Trusted Hosts: OFF

Theme Mode: **Use Global Theme** Use Own Theme

Meta Fields >

Advanced Options >

3. Set *Theme Mode* to *Use Own Theme*.
4. From the *User Theme* menu, select a theme.

**New Administrator**

User Name: Admin

Avatar: + Change Photo - Remove Photo

Comments:

Admin Type: LOCAL

New Password:

Confirm Password:

Admin Profile: Restricted\_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify

JSON API Access: None

Trusted Hosts: OFF

Theme Mode: Use Global Theme **Use Own Theme**

User Theme

|                    |         |                |               |
|--------------------|---------|----------------|---------------|
| Blueberry          | Kiwi    | Cherry         | Plum          |
| Spring             | Summer  | Autumn         | Winter        |
| High Contrast Dark | Space   | Calla Lily     | Binary Tunnel |
| Diving             | Dreamy  | Technology     | Landscape     |
| Twilight           | Canyon  | Northern Light | Astronomy     |
| Fish               | Penguin | Mountain       | Polar Bear    |
| Parrot             | Cave    | Zebra          |               |

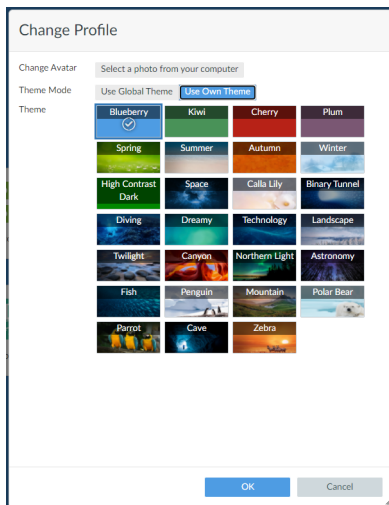
Meta Fields >

Advanced Options >

5. Click *OK*.

When a user logs into their account, they can change the theme by clicking their username, and selecting *Change Profile*.



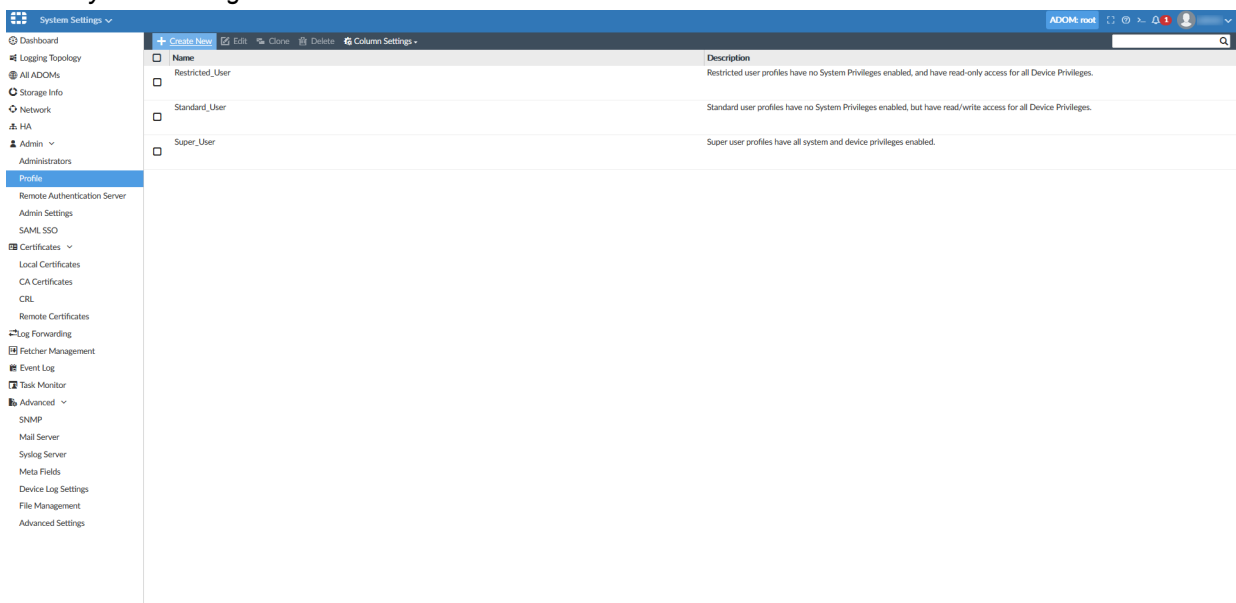


## Add operation permissions to Admin profile

FortiSoC profile permissions grant administrators access to the FortiSoC module, while preventing them from making changes to the configuration that could affect the SLA.

### To create a FortiSoC Admin profile:

1. Go to **System Settings > Admin > Profile > Create New**.



2. Configure the FortiSoC profile.
  - a. Name the profile, *Profile1*.
  - b. Set *FortSOC* to *None*.
  - c. Set *Create & Update Incidents*, *Triage Event*, *Execute Playbook*, and *Run Report* to *Read-Write*.
  - d. Click **OK**.

**New Profile**

Profile Name: Profile1

Description:

0/1023

System Settings: ☒ Read-Write ☐ Read-Only ☐ None

Administrative Domain: ☒ Read-Write ☐ Read-Only ☐ None

Device Manager: ☒ Read-Write ☐ Read-Only ☐ None

Add/Delete/Edit Devices/Groups: ☒ Read-Write ☐ Read-Only ☐ None

Log View/FortView: ☒ Read-Write ☐ Read-Only ☐ None

FortiSOC: ☐ Read-Write ☐ Read-Only ☒ None

Create & Update Incidents: ☒ Read-Write ☐ Read-Only ☐ None

Triage Event: ☒ Read-Write ☐ Read-Only ☐ None

Execute Playbook: ☒ Read-Write ☐ Read-Only ☐ None

Reports: ☐ Read-Write ☐ Read-Only ☒ None

Run Report: ☒ Read-Write ☐ Read-Only ☐ None

FortiFabric: ☒ Read-Write ☐ Read-Only ☐ None

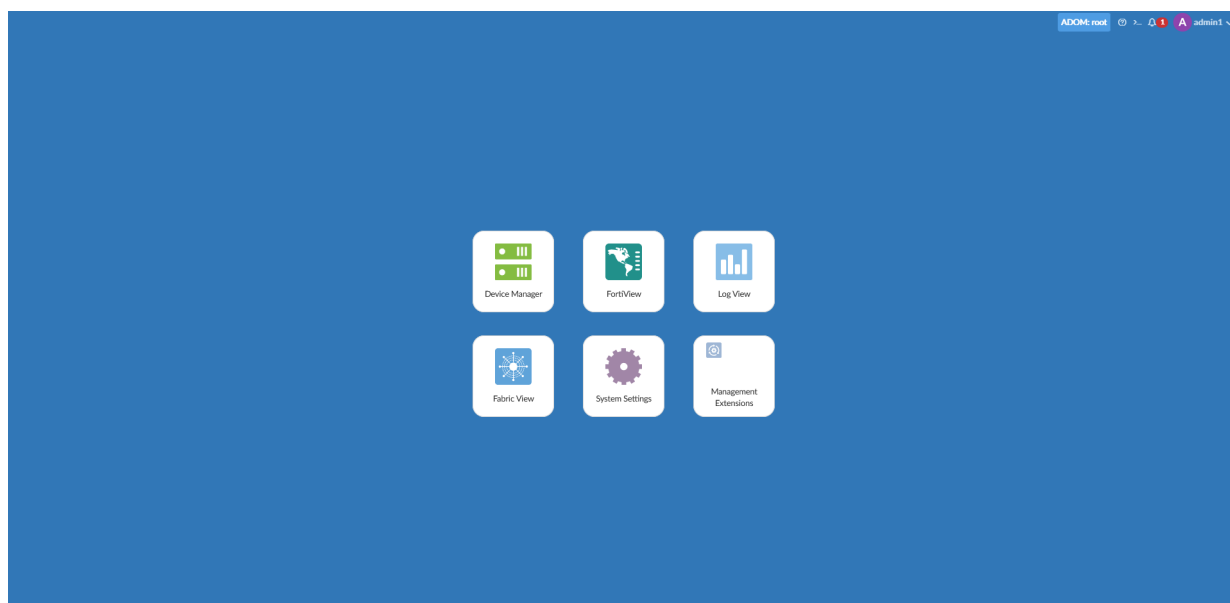
Privacy Masking: ☐ OFF

OK Cancel

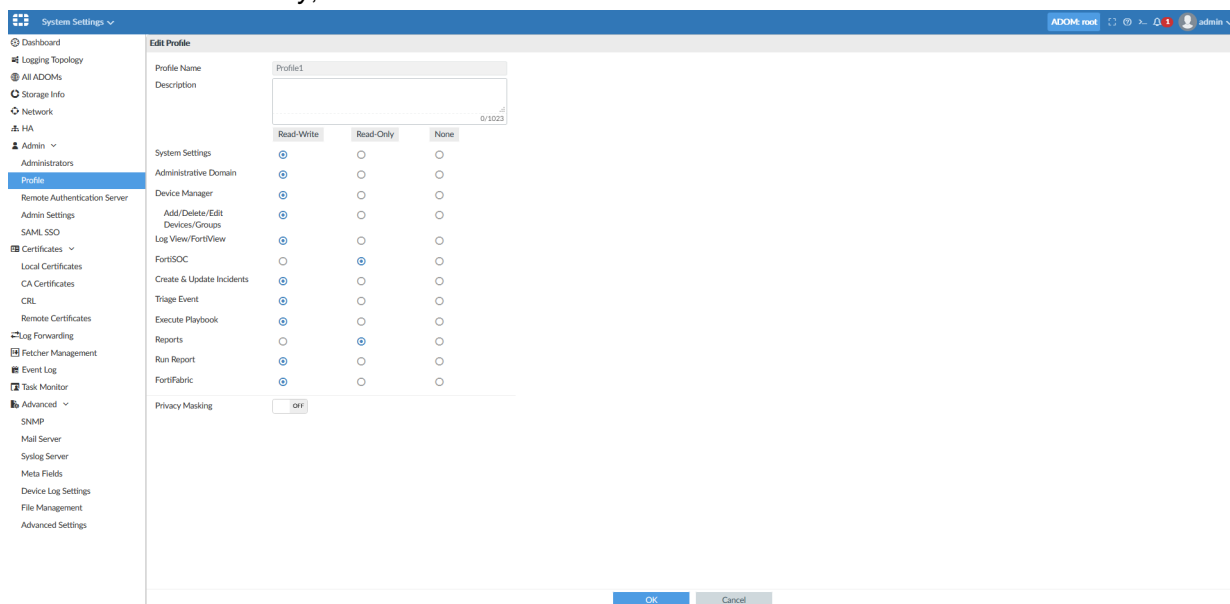
3. Apply the profile to an administrator account.
  - a. Go to *System Settings > Admin > Administrators > Create New*.
  - b. Name the new profile *Admin1*, and then select *Profile1* from the *Admin Profile* dropdown.
  - c. Click **OK**.

| Name  | Type  | Profile    | JSON API Access | ADOMs     | Trusted IPv4 Hosts |
|-------|-------|------------|-----------------|-----------|--------------------|
| admin | LOCAL | Super_User | None            | All ADOMs | 0.0.0.0/0.0.0.0    |

4. Log out of FortiAnalyzer and then log back in as *Admin1*. The FortiSoC module is not available. Log out of the account.



5. Log into FortiAnalyzer as an administrator, and go to *System Settings > Admin > Profile*.
6. Edit *Profile1*.
7. Set *FortiSOC* to *Read-Only*, and then click *OK*.



8. Log out of FortiAnalyzer, and then log back in as *Admin1*.

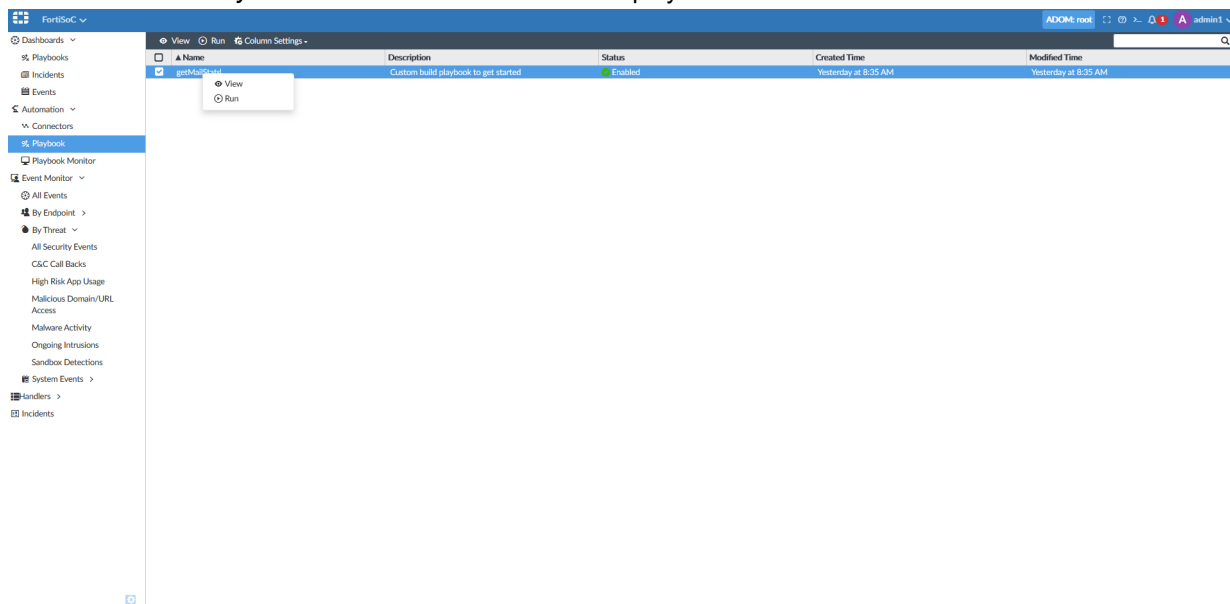
9. Go to *FortiSoC > Incidents*. You can view and create incidents.

|                                     | Incident Number | Incident Date / Time | Incident Reporter   | Incident Category | Severity            | Status | Affected Endpoint | Description |
|-------------------------------------|-----------------|----------------------|---------------------|-------------------|---------------------|--------|-------------------|-------------|
| <input type="checkbox"/>            | 1               | IN00000005           | 2021-02-08 08:43:58 | test1             | Unauthorized Access | Medium | New               | N/A         |
| <input type="checkbox"/>            | 2               | IN00000004           | 2021-02-02 15:54:02 | admin             | Unauthorized Access | Medium | New               | N/A         |
| <input type="checkbox"/>            | 3               | IN00000003           | 2021-02-02 09:51:28 | admin             | Uncategorized       | Medium | New               | N/A         |
| <input type="checkbox"/>            | 4               | IN00000002           | 2021-01-26 16:00:07 | linda             | Uncategorized       | Medium | New               | N/A         |
| <input checked="" type="checkbox"/> | 5               | IN00000001           | 2021-01-26 15:58:30 | linda             | Uncategorized       | Medium | New               | N/A         |

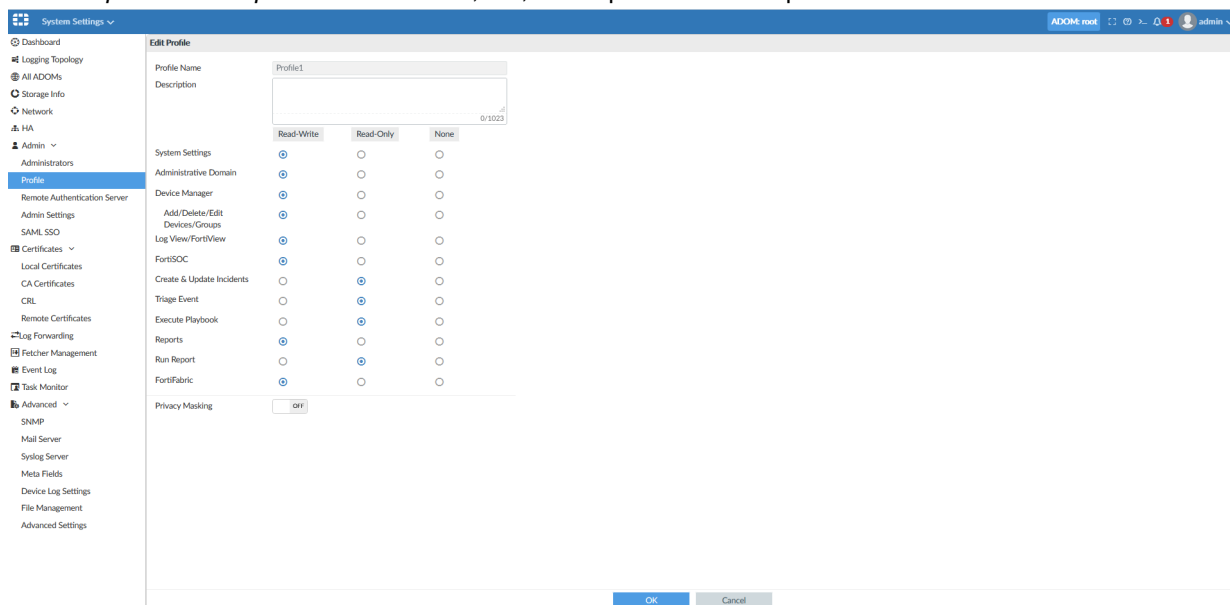
10. Go to *FortiSoC > All Events*. You can acknowledge, comment on, and create a new incident.

|                                     | Event | Event Status                        | Event Type | Count | Severity | First Occurrence    | Last Update         | Additional Info                       | Handler            | Tags           | Device Name       |
|-------------------------------------|-------|-------------------------------------|------------|-------|----------|---------------------|---------------------|---------------------------------------|--------------------|----------------|-------------------|
| <input type="checkbox"/>            | 1     | > FortiAnalyzer license limit ex... | Event      | 6     | Medium   | 7 days ago          | 38 minutes ago      | License validation state change...    | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 2     | > Device offline (11)               | Event      | 1     | Medium   | 2021-02-09 08:30:16 | 2021-02-09 08:30:16 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input checked="" type="checkbox"/> | 3     | > desc:Device offline               | Event      | 1     | Medium   | 2021-02-09 08:18:02 | 2021-02-09 08:18:02 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 4     | > desc:Device offline               | Event      | 1     | Medium   | 2021-02-08 17:44:50 | 2021-02-08 17:44:50 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 5     | > desc:Device offline               | Event      | 2     | Medium   | 2021-02-08 07:58:15 | 2021-02-08 07:58:15 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 6     | > desc:Device offline               | Event      | 2     | Medium   | 2021-02-07 22:05:06 | 2021-02-07 22:05:06 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 7     | > desc:Device offline               | Event      | 2     | Medium   | 2021-02-07 15:09:34 | 2021-02-07 15:09:34 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 8     | > desc:Device offline               | Event      | 2     | Medium   | 2021-02-06 15:09:34 | 2021-02-06 15:09:34 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 9     | > desc:Device offline               | Event      | 2     | Medium   | 2021-02-05 15:09:33 | 2021-02-05 15:09:33 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 10    | > desc:Device offline               | Event      | 1     | Medium   | 2021-02-04 15:09:33 | 2021-02-04 15:09:33 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 11    | > desc:Device offline               | Event      | 1     | Medium   | 2021-02-03 15:09:33 | 2021-02-03 15:09:33 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 12    | > desc:Device offline               | Event      | 1     | Medium   | 2021-02-02 15:09:32 | 2021-02-02 15:09:32 | Did not receive any log from d...     | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 13    | > Image upgrade                     | Event      | 6     | Medium   | A day ago           | An hour ago         | ---                                   | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 14    | > Disk quota warning (2)            | Event      | 2     | Medium   | A day ago           | 21 hours ago        | Total allocated disk quota of A...    | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 15    | > Reset to factory default (1)      | Event      | 1     | Medium   | A day ago           | A day ago           | This operation will reset all sett... | Local Device Event | System   Local | FAZ-VMJY000000003 |
| <input type="checkbox"/>            | 16    | > User login/logout failed (3)      | Event      | 4     | Medium   | 7 days ago          | A day ago           | ---                                   | Local Device Event | System   Local | FAZ-VMJY000000003 |

11. Go to *FortiSoC > Playbook*. You can now view and run a playbook.



12. Go to *Reports > All Reports*. You can view, run, and export FortiSoC reports.



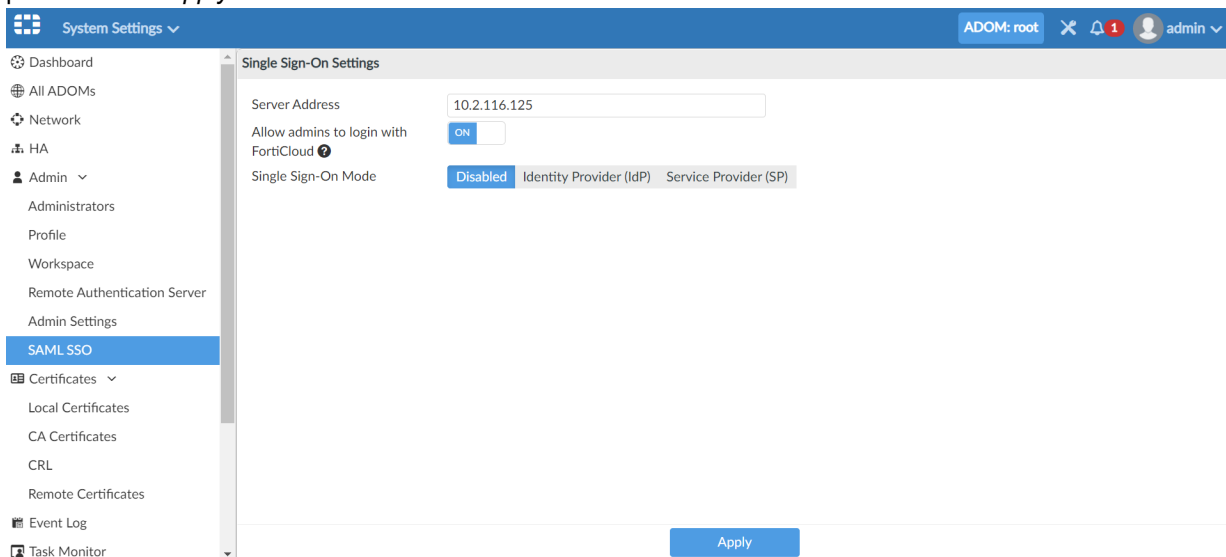
## Admins can use a SAML SSO FortiCloud account to log in to FortiAnalyzer

Admins can use SAML SSO through their FortiCloud account to log in to FortiAnalyzer.

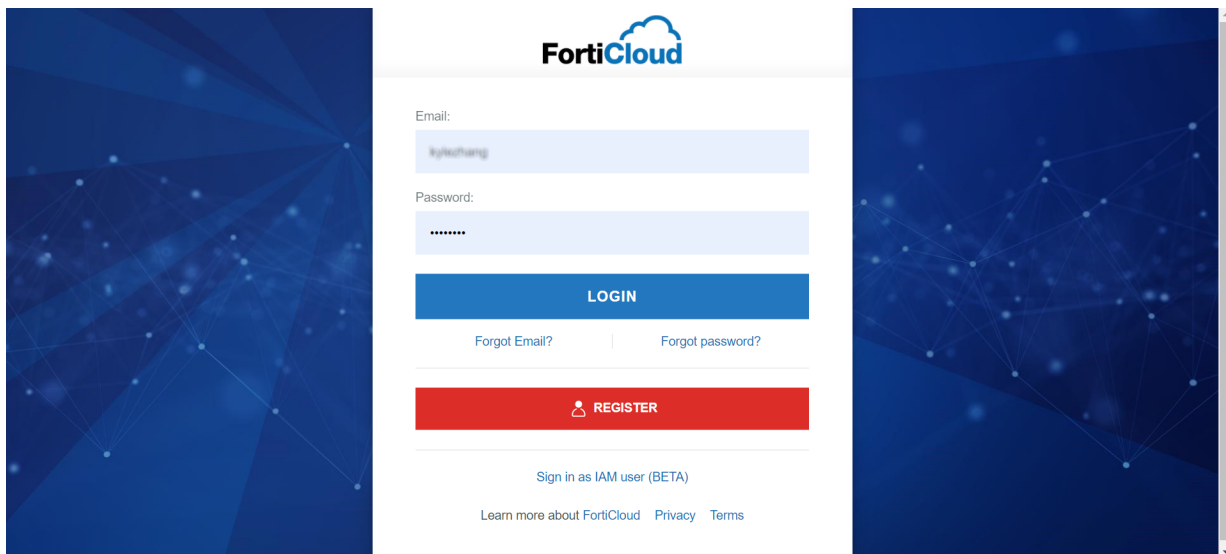
### To enable SAML SSO using FortiCloud:

1. By default, administrators can only log in using a local or remote user account configured on FortiAnalyzer.
2. To enable SAML SSO using FortiCloud, you must first register your FortiAnalyzer on [FortiCloud](#). You can confirm the FortiCloud registration status in *System Settings > Dashboard* under *License Information*.

3. Go to *System Settings > Admin > SAML SSO*, and set the *Allow admins to login with FortiCloud* toggle to the *ON* position. Click *Apply*.



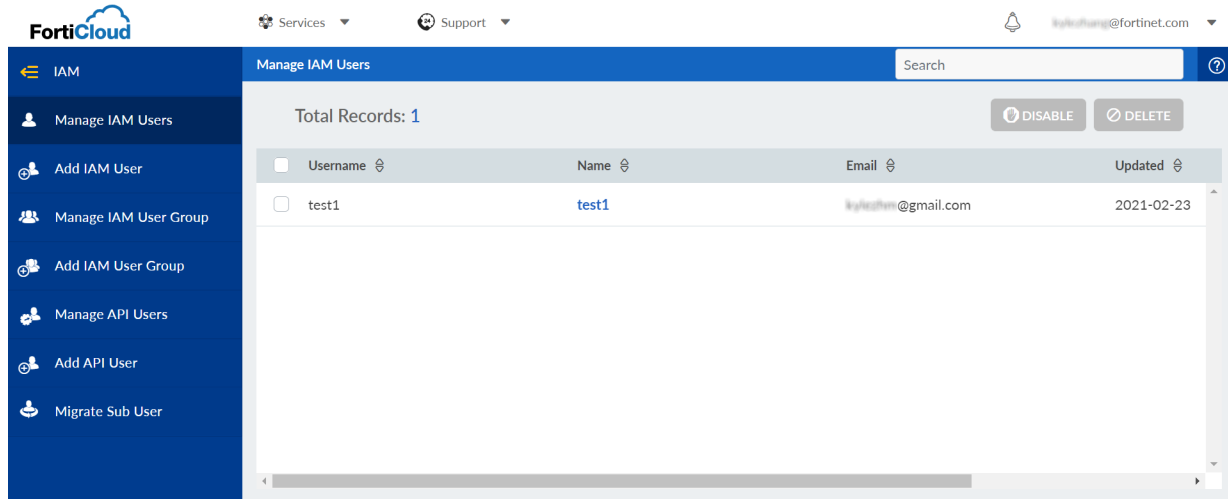
4. Sign out of FortiAnalyzer and return to the login page.  
You can now see a new option to log in using your FortiCloud account.
5. Click *Login with FortiCloud* and you are redirected to the FortiCloud login portal. Enter your FortiCloud credentials, and click *LOGIN*.



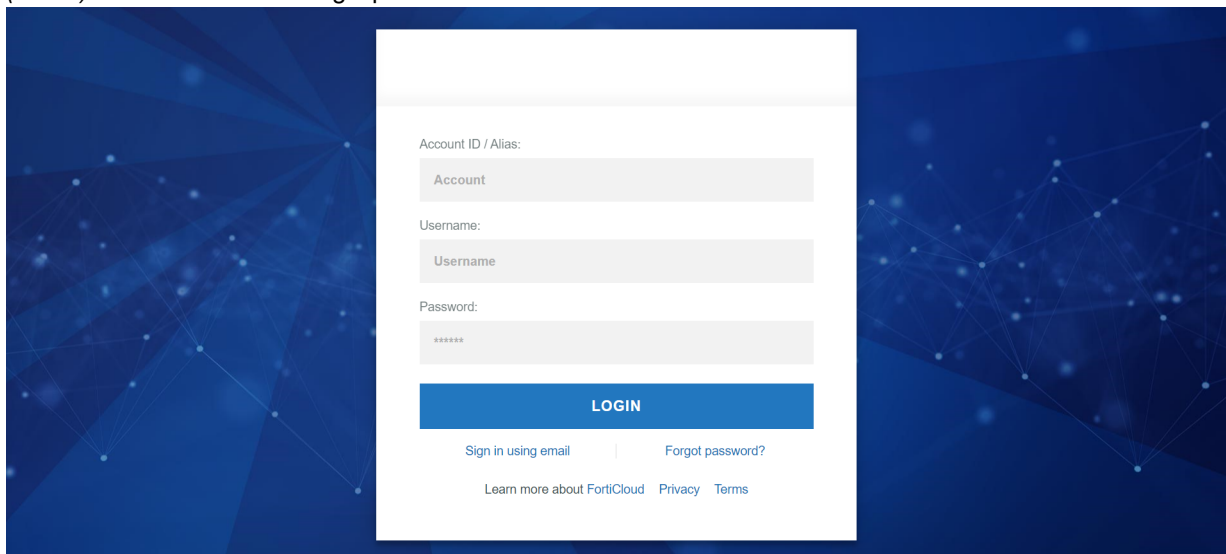
You are logged in to FortiAnalyzer with your FortiCloud account.

By default, only the account ID which the FortiAnalyzer is registered to can be used to log in to FortiAnalyzer. To enable login for additional user accounts using FortiCloud, you can configure multiple IAM users in FortiCloud.

6. Go to FortiCloud and create one or more IAM users. For more information on creating an IAM user, see [Identity & Access Management \(IAM\)](#).



7. Go to the FortiAnalyzer sign in page and click *Login with FortiCloud*, and click the option to *Sign in as IAM user (BETA)* at the bottom of the login portal.



8. Enter your IAM user credentials, and you will be logged in to FortiAnalyzer as the IAM user.

## ADOM

This section lists the new features added to FortiAnalyzer for ADOMs:

- [Support for link aggregation on page 92](#)

## Support for link aggregation

Interface link-aggregation is now supported on high-end FortiAnalyzer appliances and VM platforms to provide interface redundancy and load balance.



This feature is only available in high-end FortiAnalyzer devices (FAZ2000E and above), and VM platforms.

### To create an aggregate interface in the GUI:

1. Go to *System Settings > Network*.
2. In the toolbar, click *Create New*. The *Create New Interface* window opens.

3. In the *Name* field, enter a name for the interface (for example, Aggregation1)



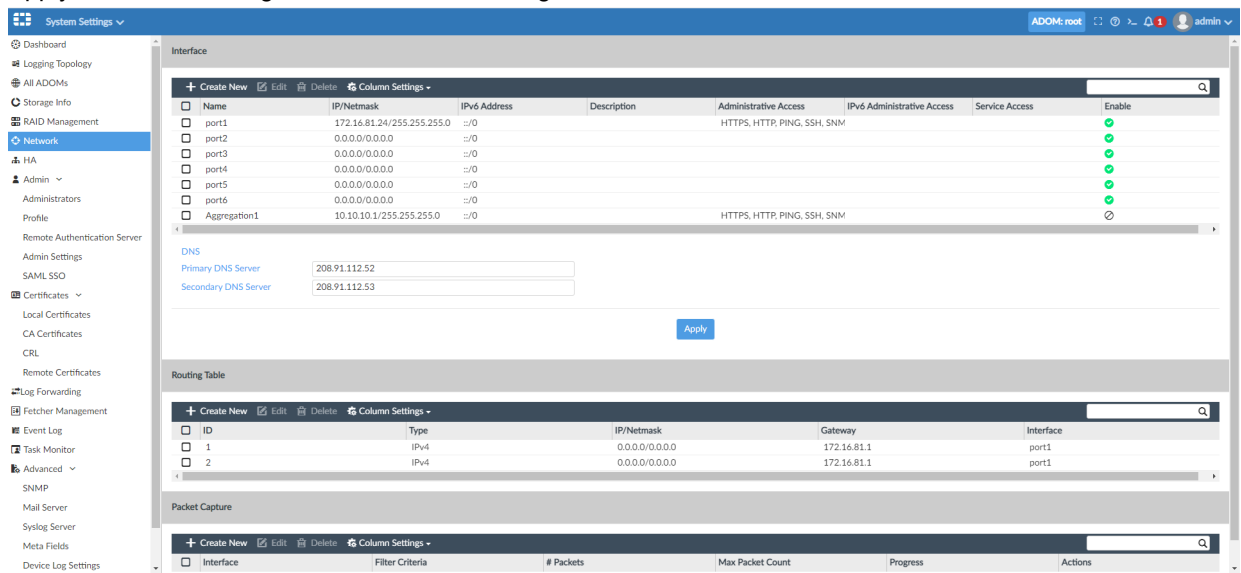
4. Click the *Members* field to select the available ports.

The screenshot shows the 'Create New Interface' window in FortiAnalyzer. The 'Name' field is 'AggregateInterface1'. The 'Type' is 'Aggregate'. The 'Members' field is selected, showing a list of available ports: port1, port5, and port6. The 'IP Address/Netmask' field is empty. The 'Administrative Access' field has checkboxes for HTTPS, HTTP, PING, SSH, SNMP, and Web Service. The 'IPv6 Administrative Access' field has checkboxes for HTTPS, HTTP, PING, SSH, SNMP, and Web Service. The 'LACP Speed' is set to 'Fast'. The 'Minimum Links Up' is set to '1'. The 'Minimum Links Down' is set to 'Operational'. The 'Links Up Delay' is set to '50' (milliseconds). The 'OK' and 'Cancel' buttons are at the bottom right.

5. In the *IP Address/Netmask* field, enter a minimum of two IP addresses. At least two ports need to be up for the aggregate interface to work.

The screenshot shows the 'Create New Interface' window in FortiAnalyzer. The 'Name' field is 'AggregateInterface1'. The 'Type' is 'Aggregate'. The 'Members' field is selected, showing a list of available ports: port1, port5, and port6. The 'IP Address/Netmask' field is filled with '10.10.10.1/255.255.255.0'. The 'Administrative Access' field has checkboxes for HTTPS, HTTP, PING, SSH, SNMP, and Web Service. The 'IPv6 Administrative Access' field has checkboxes for HTTPS, HTTP, PING, SSH, SNMP, and Web Service. The 'LACP Speed' is set to 'Fast'. The 'Minimum Links Up' is set to '2'. The 'Minimum Links Down' is set to 'Operational'. The 'Links Up Delay' is set to '50' (milliseconds). The 'OK' and 'Cancel' buttons are at the bottom right.

## 6. Apply the default settings for the rest of the configurations.



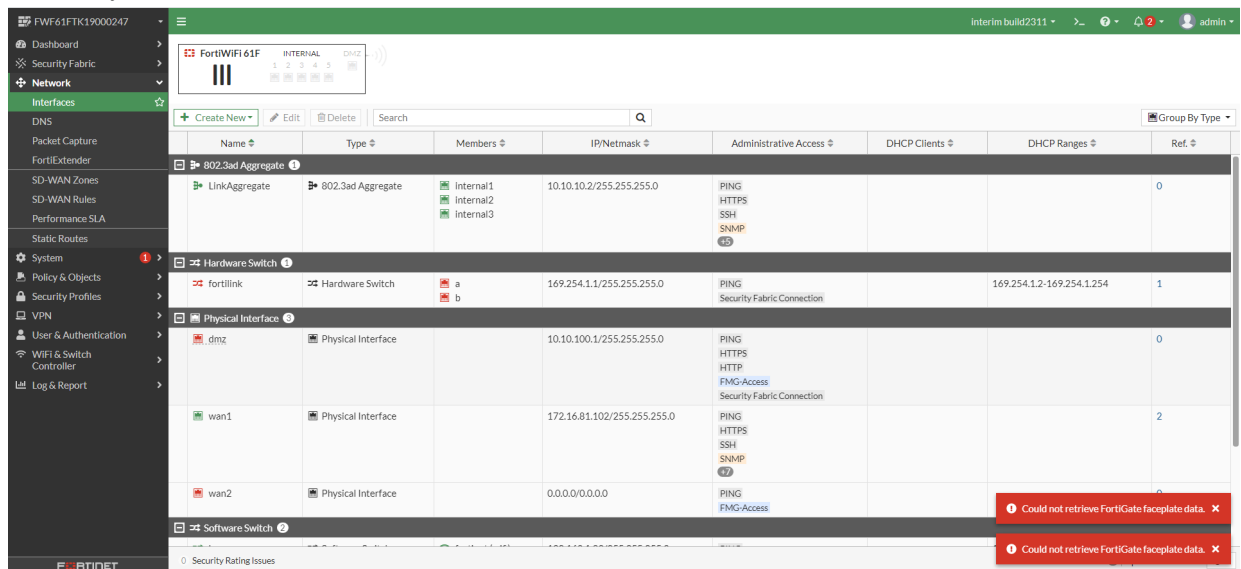
## 7. Click OK. The aggregation interface is created.

### To verify the aggregation interface is up with the CLI:

```
FAZ3000F # config system interface
(interface)# edit Aggregation1
(Aggregation1)# set status up
(Aggregation1)# end
FAZ3000F #
```

### To configure the aggregation interface in FortiGate:

1. In FortiGate go to *Network > Interfaces*, and configure the aggregation interface using the same subnet as FortiAnalyzer.



2. Go to **Log & Report > Log Settings**, and configure the logs sent to FortiAnalyzer through the aggregation interface.

The screenshot displays the FortiGate Log Settings interface. The left sidebar shows the navigation menu with 'Log & Report' selected. The main content area is titled 'Log Settings' and includes a 'Historical Disk Usage' graph showing disk usage over time. Below the graph, the 'Remote Logging and Archiving' section is configured with the following settings:

- Send logs to FortiAnalyzer/FortiManager: **Enabled** (with a red 'Disabled' button)
- IP address: 10.10.10.1 (with a 'Test Connectivity' button)
- Connection status: **Connected**
- Storage usage: 35.98 MIB / 50.00 GIB
- Analytics usage: 34.56 MIB / 35.00 GIB
- Archive usage: 1.41 MIB / 15.00 GIB
- Upload option: **Real Time** (with 'Every Minute' and 'Every 5 Minutes' options)
- Allow access to FortiGate REST API: ☒
- Verify FortiAnalyzer certificate: ☐

The 'Additional Information' section on the right includes links for 'API Preview', 'Edit in CLI', 'FortiAnalyzer', 'Configure Multiple FortiAnalyzers on a Multi-VDOM FortiGate', 'Documentation', 'Online Help', 'Video Tutorials', and 'Security Rating Issues'.

3. In FortiAnalyzer, go to **Device Manager** to confirm FortiGate has established a connection with FortiAnalyzer through the aggregation interface.

The screenshot displays the FortiAnalyzer Device Manager interface. The top bar shows '1 Devices Total' and '2 Devices Unauthorized'. The table below lists the connected devices:

| Device Name     | IP Address | Platform      | Logs      | Average Log Rate(Logs/Sec) | Device Storage | Description | Firmware Version          |
|-----------------|------------|---------------|-----------|----------------------------|----------------|-------------|---------------------------|
| FW61FTK19000247 | 10.10.10.2 | FortiWiFi-61F | Real Time | N/A                        | (0%)           |             | FortiGate 6.6.0 (Interim) |

# Management Extensions

This section lists the other new features added to FortiAnalyzer for management extensions:

- [New management extension - FortiSOAR on page 96](#)

## New management extension - FortiSOAR

This feature adds the FortiSOAR application as a management extension application (MEA). FortiSOAR is an enterprise-built security orchestration and security automation workbench that empowers security operation teams.

By default, FortiSOAR MEA is disabled. You can enable FortiSOAR MEA by using the GUI or the CLI.

There are minimum system resources recommended for FortiAnalyzer when using FortiSOAR MEA. See the FortiAnalyzer Release Notes for additional information.

The following CLI commands are available for FortiSOAR MEA:

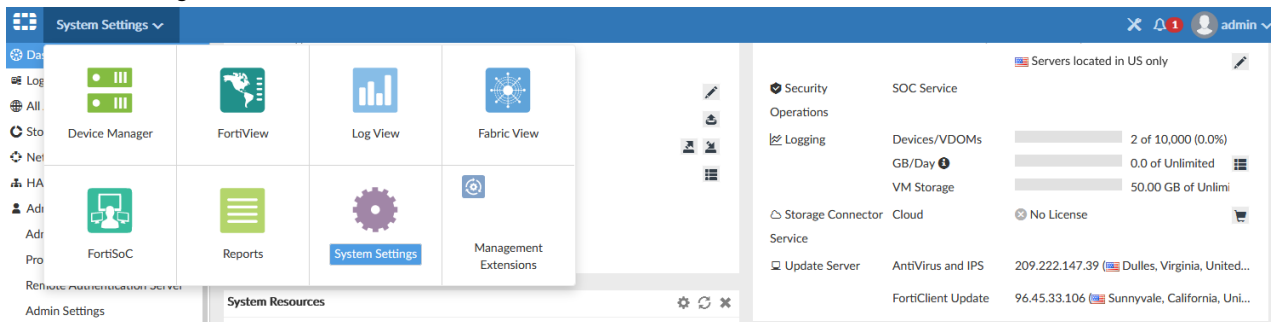
- `config system docker`
- `diagnose docker status`
- `diagnose docker upgrade fortisoar`



FortiAnalyzer supports only FortiSOAR MEA. Although you can use the CLI to enable additional management extension applications, they are not supported by FortiAnalyzer. Enabled, unsupported management extension applications are hidden from the FortiAnalyzer GUI, but still consume valuable resources. Be sure to only enable FortiSOAR MEA on FortiAnalyzer when using the CLI.

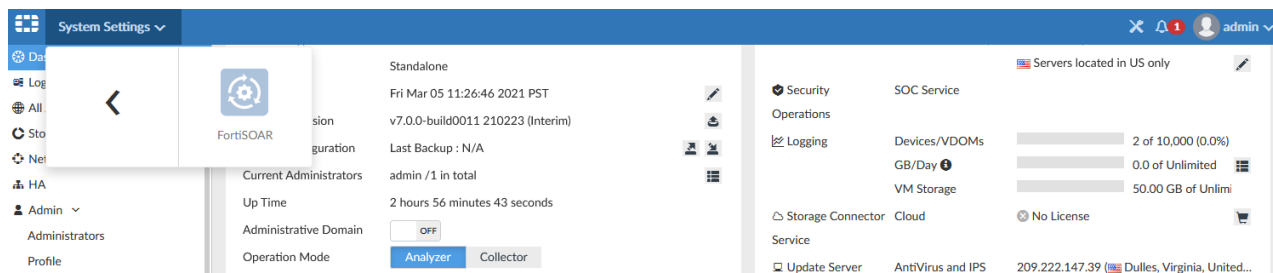
### To enable FortiSOAR MEA by using the GUI:

1. Go to the *Management Extensions* tile.



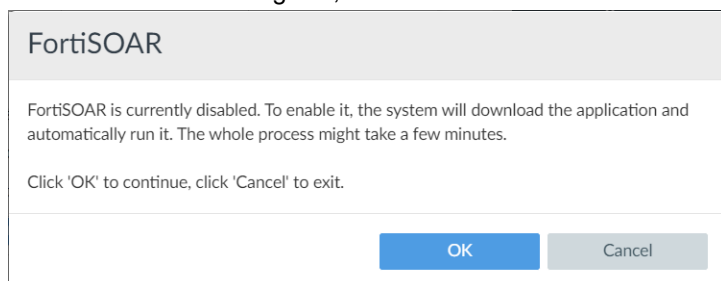
The management extension application options are displayed.

2. Click *FortiSOAR*.



A confirmation dialog box is displayed.

3. In the confirmation dialog box, click *OK*.

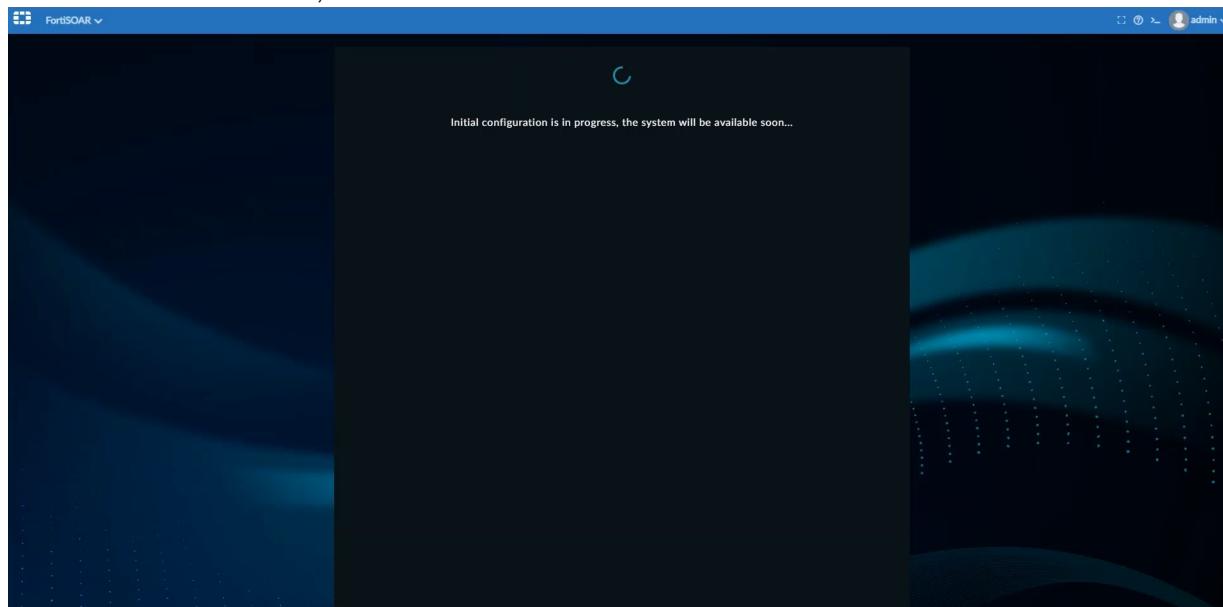


FortiSOAR MEA is downloaded from the Fortinet registry (registry.fortinet.com).

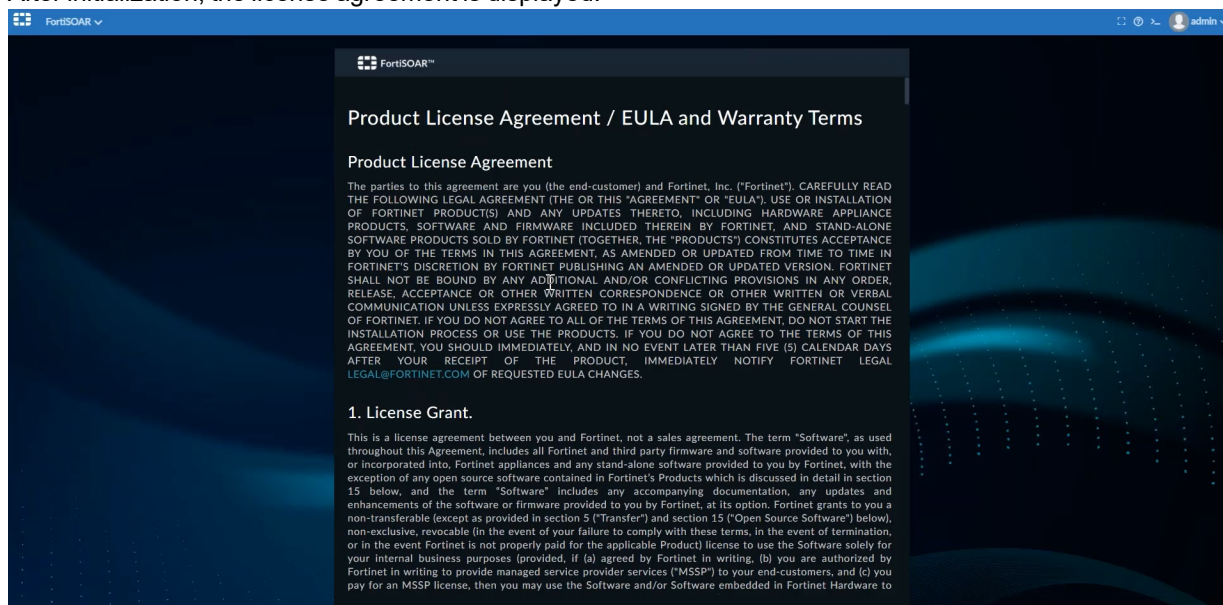
A progress bar displays under the FortiSOAR tile.



After FortiSOAR downloads, it initializes.

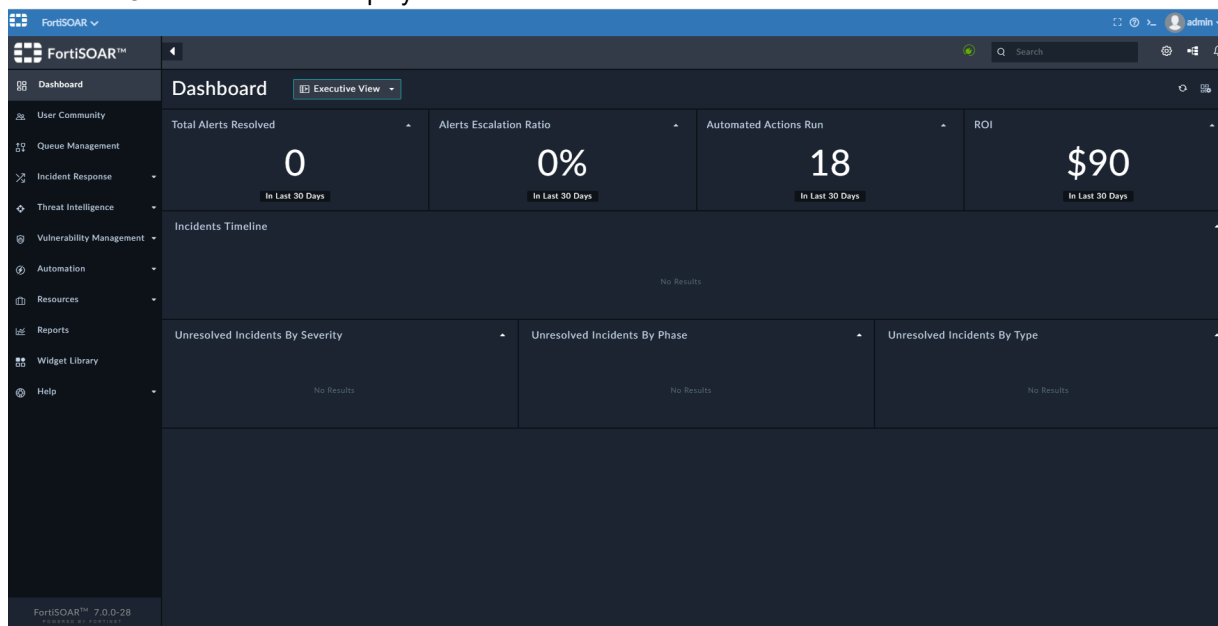


After initialization, the license agreement is displayed.

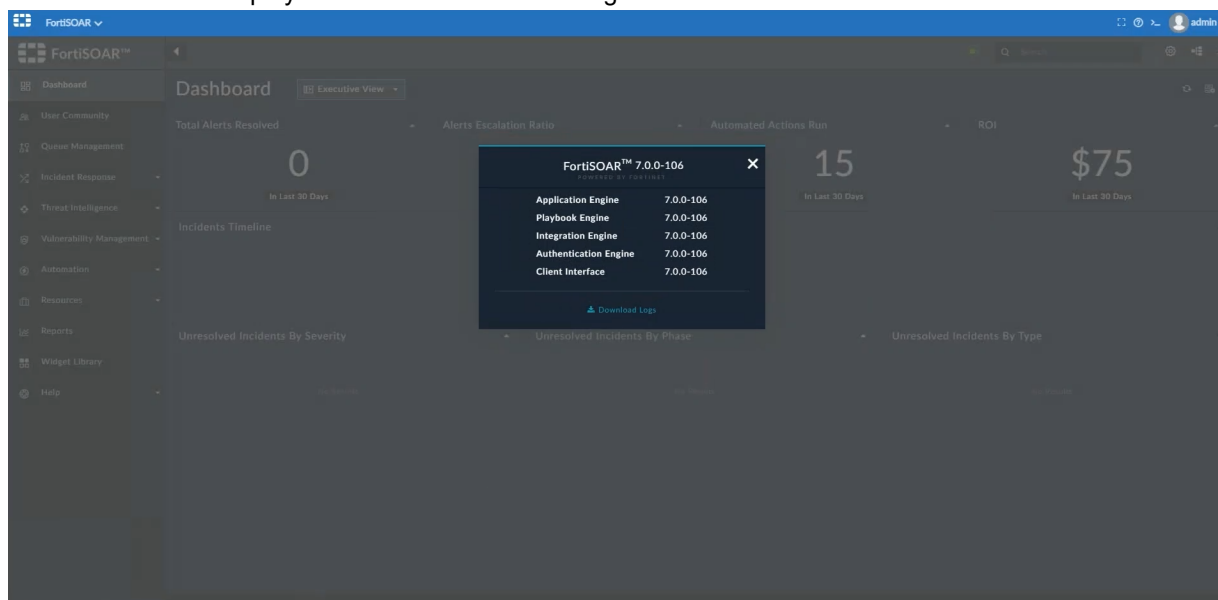


4. Read the license agreement, and click *Agree*.

- Log in to FortiSOAR by using your FortiAnalyzer login.  
The FortiSOAR dashboard is displayed.



The version and build information for FortiSOAR can be found on the bottom-left corner of the Dashboard. Clicking on this information displays the version and build dialog.



# Other

This section lists the other new features added to FortiAnalyzer:

- [FortiAnalyzer Setup wizard on page 100](#)
- [FortiAnalyzer VM licenses on page 104](#)
- [CSF support for multiple VDOMs on page 117](#)
- [FortiAnalyzer Federation on page 110](#)

## FortiAnalyzer Setup wizard

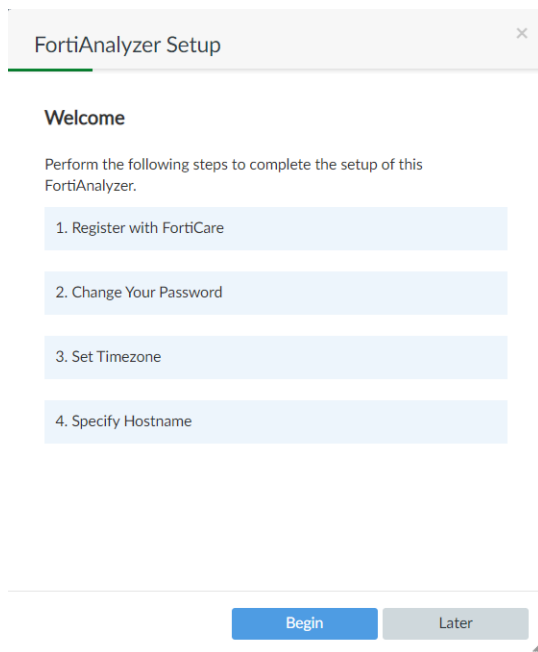
The FortiAnalyzer Setup wizard lets you register with FortiCare as well as perform the following actions:

- Registering with FortiCare
- Changing your password
- Setting the time zone
- Specifying a hostname

When an action is complete, a green checkmark displays it in the wizard, and the wizard no longer displays after you log in to FortiAnalyzer.

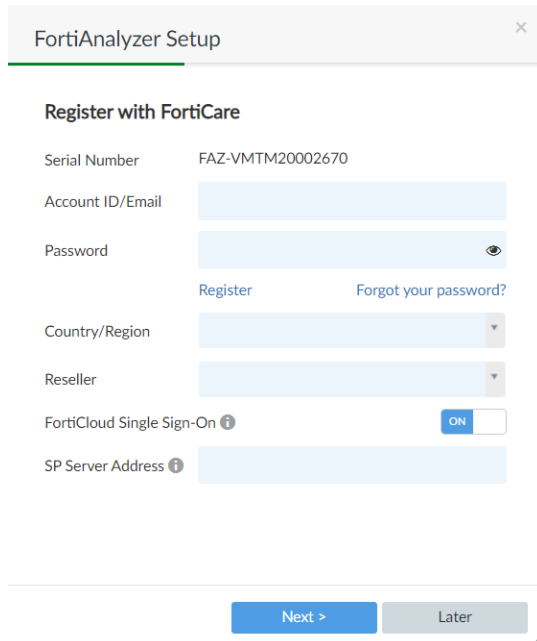
### To use the FortiAnalyzer Setup wizard:

1. Log in to FortiAnalyzer.  
The *FortiAnalyzer Setup* dialog box is displayed.





2. Click *Begin* to start the setup process now.  
Alternately, click *Later* to postpone the setup tasks.
3. When prompted, register with FortiCare.

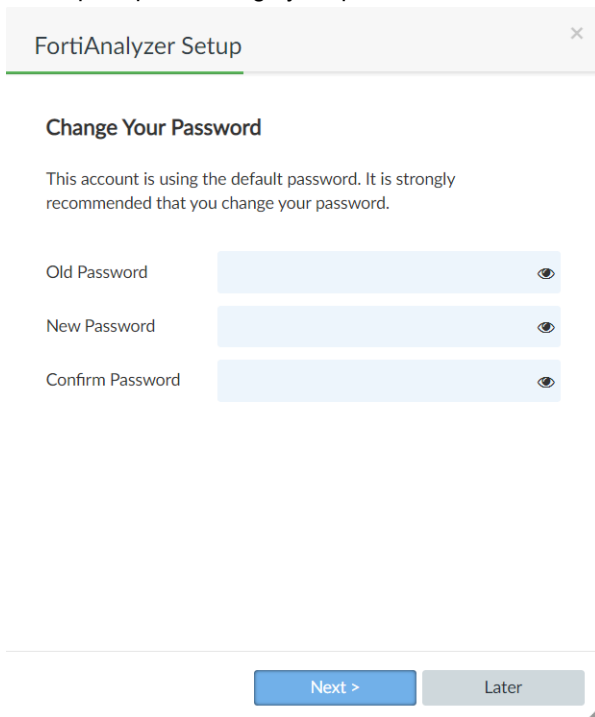


The screenshot shows a 'FortiAnalyzer Setup' dialog box with a close button (X) in the top right corner. The main heading is 'Register with FortiCare'. Below this, there are several input fields and a toggle switch:

- Serial Number:** Pre-filled with 'FAZ-VMTM20002670'.
- Account ID/Email:** An empty text input field.
- Password:** An empty password input field with an eye icon for toggling visibility.
- Below the Password field are two links: 'Register' and 'Forgot your password?'.
- Country/Region:** A dropdown menu.
- Reseller:** A dropdown menu.
- FortiCloud Single Sign-On:** A toggle switch currently set to 'ON'.
- SP Server Address:** An empty text input field with an information icon (i) to its left.

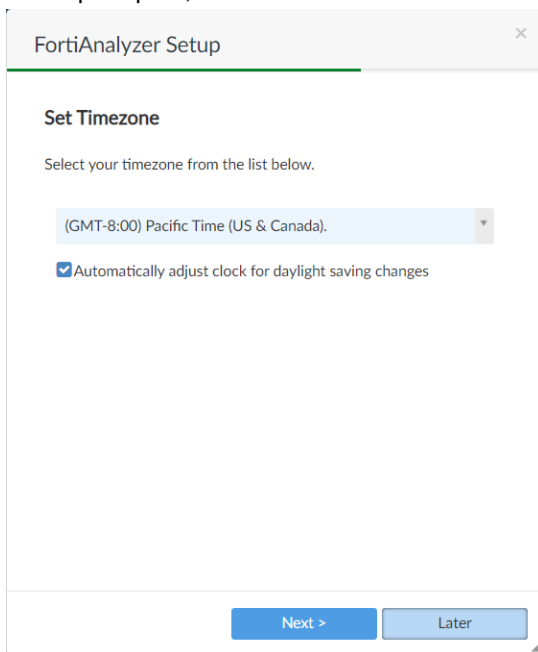
At the bottom of the dialog box, there are two buttons: 'Next >' (highlighted in blue) and 'Later' (greyed out).

- a. In the *Account ID/Email* box, type your FortiCare account ID or email.  
If you do not yet have a FortiCare account, click *Register* to create a new account.
- b. In the *Password* box, type your FortiCare password.  
If you have forgotten your FortiCare password, click *Forgot your password* to proceed through the password recovery process.
- c. In the *Country/Region* box, select your country or region from the dropdown.
- d. In the *Reseller* box, select your reseller from the dropdown.
- e. Set the *FortiCloud Single Sign-On* toggle to the *ON* or *OFF* position to enable or disable FortiCloud SSO sign on.  
When enabled, you must also enter the *SP Server Address*.
- f. Click *Next*.

**4. When prompted, change your password.**

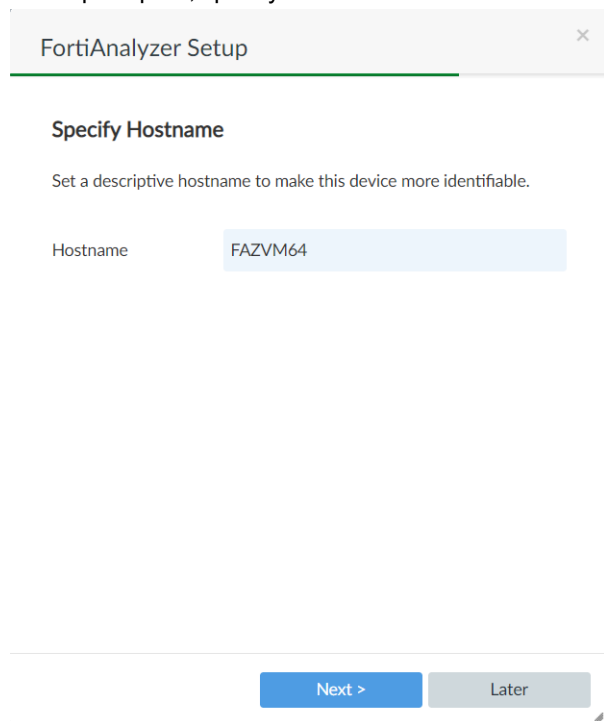
The screenshot shows a 'FortiAnalyzer Setup' dialog box with a close button (X) in the top right corner. The title is 'FortiAnalyzer Setup'. Below the title bar, the section is 'Change Your Password'. A message states: 'This account is using the default password. It is strongly recommended that you change your password.' There are three input fields: 'Old Password', 'New Password', and 'Confirm Password', each with a password icon (eye) to its right. At the bottom, there are two buttons: 'Next >' (highlighted in blue) and 'Later' (grey).

- a. In the *Old Password* box, type the old password.
- b. In the *New Password* box, type the new password.
- c. In the *Confirm Password* box, type the new password again.
- d. Click *Next*.

**5. When prompted, set the time zone.**

The screenshot shows a 'FortiAnalyzer Setup' dialog box with a close button (X) in the top right corner. The title is 'FortiAnalyzer Setup'. Below the title bar, the section is 'Set Timezone'. A message states: 'Select your timezone from the list below.' There is a dropdown menu showing '(GMT-8:00) Pacific Time (US & Canada)'. Below the dropdown, there is a checkbox labeled 'Automatically adjust clock for daylight saving changes' which is checked. At the bottom, there are two buttons: 'Next >' (highlighted in blue) and 'Later' (grey).

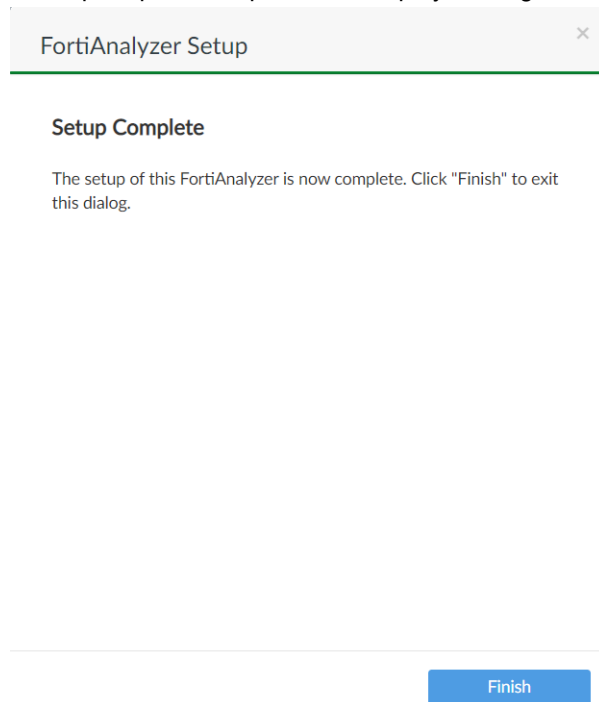
- a. From the list, select the time zone.
  - b. (Optional) Clear the *Automatically adjust clock for daylight savings changes* checkbox if desired.  
By default FortiAnalyzer is configured to automatically adjust closed for daylight savings.
  - c. Click *Next*.
6. When prompted, specify the hostname.



The screenshot shows a 'FortiAnalyzer Setup' dialog box with a close button (X) in the top right corner. The title bar is 'FortiAnalyzer Setup'. Below the title bar, the section is 'Specify Hostname'. A descriptive text says 'Set a descriptive hostname to make this device more identifiable.' Below this, there is a label 'Hostname' and a text input field containing 'FAZVM64'. At the bottom of the dialog, there are two buttons: 'Next >' (highlighted in blue) and 'Later' (greyed out).

- a. In the *Hostname* box, type a hostname.
- b. Click *Next*.

7. When prompted, complete the setup by clicking *Finish*.



You are logged in to FortiAnalyzer.

## FortiAnalyzer VM licenses

For FortiAnalyzer virtual machines (VMs), you can use the FortiAnalyzer GUI to:

- Request and activate a trial license
- Activate a perpetual or VM-S license
- Activate an add-on perpetual or VM-S license

FortiAnalyzer must be able to access the Internet to communicate with FortiCloud to complete the licensing process.

The licensing process requires you to log in to FortiCloud. If you do not have a FortiCloud account, you can create one to complete the licensing process.

This topic contains the following sections:

- [Requesting and activating a trial license on page 104](#)
- [Activating a new license on page 107](#)
- [Activating an add-on license on page 108](#)

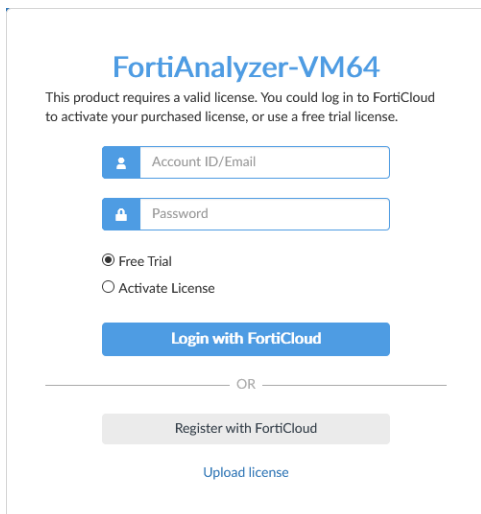
Some of the screen shots in the following examples are for FortiManager, but the process applies to both FortiManager and FortiAnalyzer.

## Requesting and activating a trial license

You can use the FortiAnalyzer GUI to request and activate a trial license for a FortiAnalyzer VM.

**To request and activate a trial license:**

1. In a browser, access the IP address for the FortiAnalyzer GUI.  
The login dialog box is displayed.

The image shows the FortiAnalyzer-VM64 login dialog box. At the top, it says "FortiAnalyzer-VM64" in blue. Below that, a message states: "This product requires a valid license. You could log in to FortiCloud to activate your purchased license, or use a free trial license." There are two input fields: "Account ID/Email" and "Password", each with a blue icon on the left. Below these fields are two radio buttons: "Free Trial" (selected) and "Activate License". A blue button labeled "Login with FortiCloud" is positioned below the radio buttons. Below this button is a horizontal line with "OR" in the center. Under the line is a gray button labeled "Register with FortiCloud". At the bottom, there is a blue link labeled "Upload license".

2. Select *Free Trial*, and click *Login with FortiCloud*.  
If you do not have a FortiCloud account, click *Register with FortiCloud* to create one.  
The *Free Trial License Agreement* is displayed.

## Free Trial License Agreement



### FortiAnalyzer-VM/FortiManager-VM Free Limited License Agreement

#### TERMS AND CONDITIONS

THESE TERMS AND CONDITIONS APPLY BETWEEN THE ENTITY SET FORTH BELOW (THE "CUSTOMER") AND FORTINET, WHERE BOTH PARTIES CONSENT TO BE BOUND BY THESE TERMS AND CONDITIONS UNDER THIS FREE LIMITED LICENSE AGREEMENT (THE "AGREEMENT"). IF YOU DO NOT AGREE TO THE TERMS, YOU SHOULD NOT ACCEPT THE AGREEMENT AND SHOULD CONTACT [LEGAL@FORTINET.COM](mailto:LEGAL@FORTINET.COM) TO REQUEST CHANGES TO THE AGREEMENT

#### 1) FREE LIMITED LICENSE AGREEMENT.

This Agreement is made for the purpose of testing and evaluating Fortinet's FortiAnalyzer and FortiManager Virtual Machine which have limited features as compared to the full version (hereinafter the "Products") for their potential purchase. Although the Products will have limited features (as detailed below), they will allow Customer to determine if they perform to specifications and expectations.

#### 2) PERMITTED USES AND RESTRICTIONS FOR THE LICENSE.

Fortinet grants Customer a nonexclusive, and nontransferable, limited license to use the Products for testing and evaluation (either by Customer or a third party evaluator). Customers will be provided with 1 limited free trial of the Products with their FortiCare account. The Products will include a maximum of 1 GB/day logs, 3 devices, 2 ADOMs, and do not include services or support, such as FortiCare (support and maintenance) or FortiGuard (subscription services). Customer may use the Products for management and analytics of data generated by other Fortinet products. The trial license does not come with any obligation or promise by Fortinet to provide FortiCare (support and maintenance) or FortiGuard (subscription services). Customer's access and use of the Products are subject to the limitations of their respective trial versions and are subject to all of Fortinet's applicable the terms and conditions, including Fortinet's then current End User License Agreement ("EULA") which can be found at: <http://www.fortinet.com/doc/legal/EULA.pdf> and Fortinet Service Terms and Conditions ("Terms of Service") which can be found at <https://www.fortinet.com/content/dam/fortinet>

☒ I have read and accept the terms in the License Agreement.

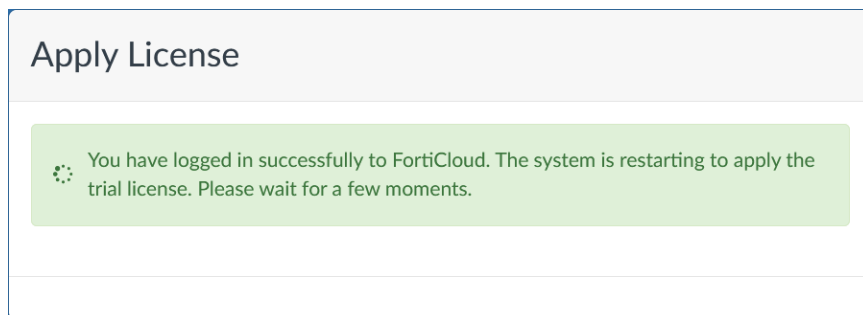
Accept

Cancel

### 3. Accept the license agreement:

- a. Read the license agreement.
- b. Select the *I have read and accept the terms in the License Agreement* checkbox.
- c. Click *Accept*.

The license is applied, and you are logged in to FortiAnalyzer.



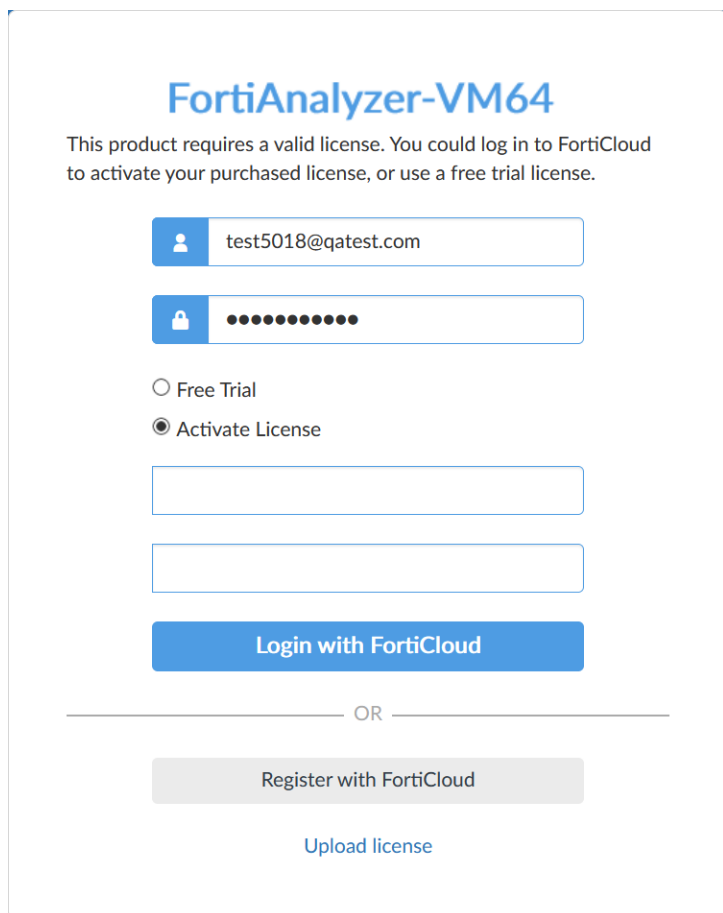
4. Go to *System Settings > Dashboard > License Information* widget.  
The *VM License* option displays *Trial License*.

## Activating a new license

You can use the FortiAnalyzer GUI to activate a new license for virtual machines. Licenses for VM-S subscriptions and perpetual subscriptions are supported.

### To activate a new license:

1. In a browser, access the IP address for the FortiAnalyzer GUI.  
The login dialog box is displayed.



2. Select *Activate License*, enter your license key, and click *Login with FortiCloud*. The *License Agreement* is displayed.

License Agreement

Fortinet

**Fortinet Service Terms & Conditions**  
For FortiCare, FortiGuard and other Fortinet Service Offerings

THESE TERMS AND CONDITIONS APPLY TO THE PROVISION OF SERVICES BY FORTINET AND EXCLUSIVELY GOVERN THE LEGAL RELATIONSHIP BETWEEN YOU (THE "CUSTOMER") AND FORTINET. IT SETS FORTH THE LEGALLY BINDING RIGHTS AND OBLIGATIONS OF THE CUSTOMER IN RELATION TO FORTICARE SUPPORT OR FORTIGUARD SUBSCRIPTION SERVICES OR OTHER FORTINET SERVICE OFFERINGS. THE CUSTOMER CONSENTS TO BE BOUND BY THESE TERMS AND CONDITIONS (THE "AGREEMENT"). THE CUSTOMER REPRESENTS THAT IT IS A SOPHISTICATED ENTITY, THAT HAS READ AND UNDERSTANDS THIS AGREEMENT AND HAS HAD SUFFICIENT OPPORTUNITY TO CONSULT WITH COUNSEL BEFORE AGREEING TO THE TERMS HEREIN. IF THE CUSTOMER DOES NOT AGREE TO THE TERMS, THE CUSTOMER SHOULD NOT ACCEPT THE AGREEMENT AND SHOULD CONTACT [LEGAL@FORTINET.COM](mailto:LEGAL@FORTINET.COM) TO REQUEST CHANGES TO THE AGREEMENT. THE CUSTOMER AGREES THAT ANY OF THE FOLLOWING ACTIONS BY CUSTOMER REPRESENTATIVES REPRESENT THE CUSTOMER'S AUTHORIZED CONSENT TO BE BOUND BY THIS AGREEMENT: (I) RECEIVING, DOWNLOADING, DEPLOYING OR USING ANY SOFTWARE PROVIDED IN CONNECTION WITH FORTINET SERVICES, (II) RECEIVING, CONFIGURING, LOGGING IN, REGISTERING OR OTHERWISE USING OR BENEFITTING FROM THE SERVICES, OR (III) BY CLICKING ON THE "ACCEPT" BUTTON UPON REGISTRATION (ANY OF (I), (II), OR (III) SHALL CONSTITUTE "ACCEPTANCE" BY CUSTOMER). THE CUSTOMER HEREBY ACKNOWLEDGES AND AGREES THAT THE PERSON ENGAGING IN (I), (II), AND/OR (III) IS AUTHORIZED TO BIND THE CUSTOMER TO THE TERMS HEREIN. FOR CLARITY, NOTWITHSTANDING ANYTHING TO THE CONTRARY, IF CUSTOMER IS USING AN AUTOREGISTRATION TOOL OR HAS ENGAGED A FORTIPARTNER OR FORTINET TO REGISTER THE SERVICE CONTRACT ON ITS BEHALF, CUSTOMER ACKNOWLEDGES AND AGREES THAT ANY AND ALL UNITS REGISTERED USING SUCH TOOL SHALL BE SUBJECT TO THIS AGREEMENT.

☒ I have read and accept the terms in the License Agreement.

Accept Cancel

3. Accept the license agreement:
  - a. Read the license agreement.
  - b. Select the *I have read and accept the terms in the License Agreement* checkbox.
  - c. Click *Accept*.

The license is applied, and you are logged in to FortiAnalyzer.
4. Go to *System Settings > Dashboard > License Information* widget. The *VM License* option displays *Valid*.

## Activating an add-on license

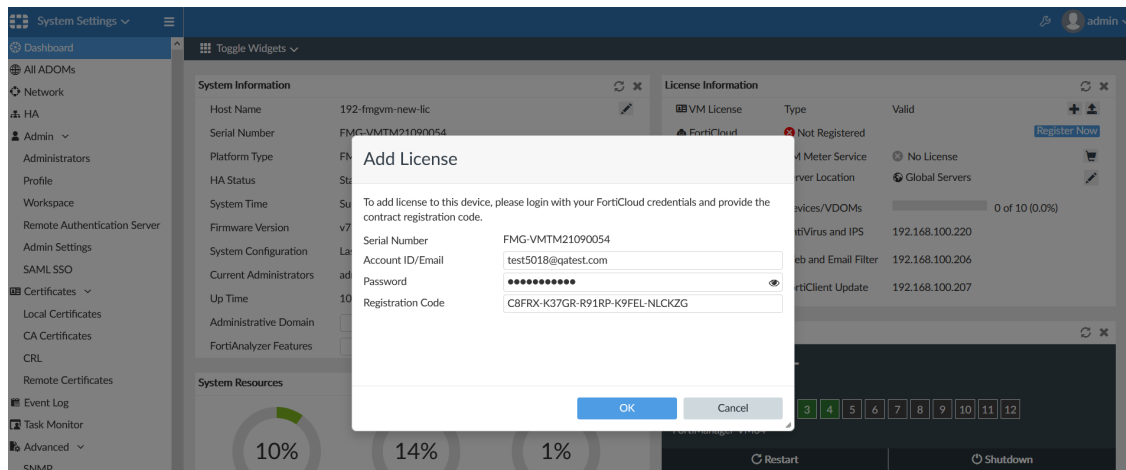
You can use the FortiAnalyzer GUI to activate an add-on license for a VM-S subscription or a perpetual subscription.

In the following example, the FortiManager VM has a base license, and you want to apply an add-on perpetual license named *1000UG*.

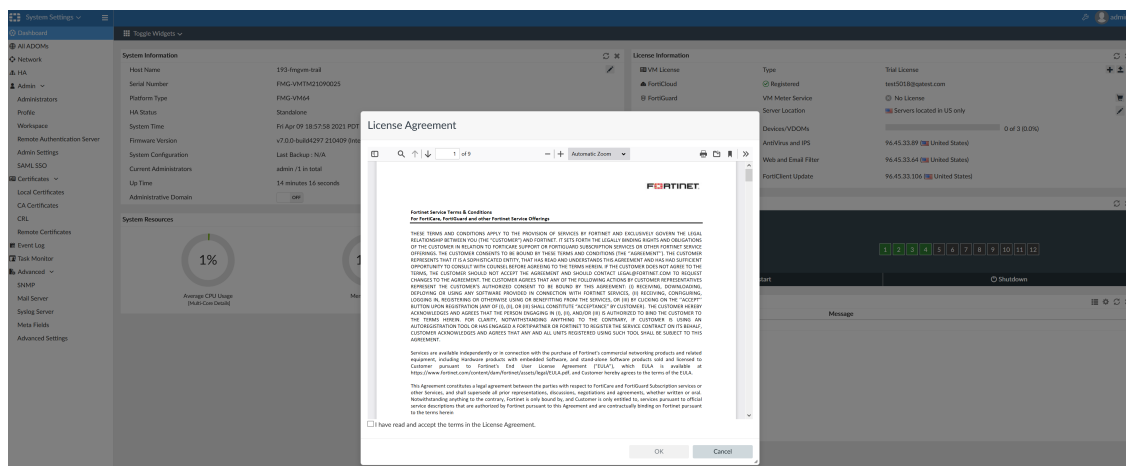
### To activate an add-on license:

1. Log in to FortiAnalyzer, and go to *System Settings > Dashboard*.
2. In the *License Information* widget, beside the *VM License* option, click the *Add License* button. The *Add License* dialog box is displayed.

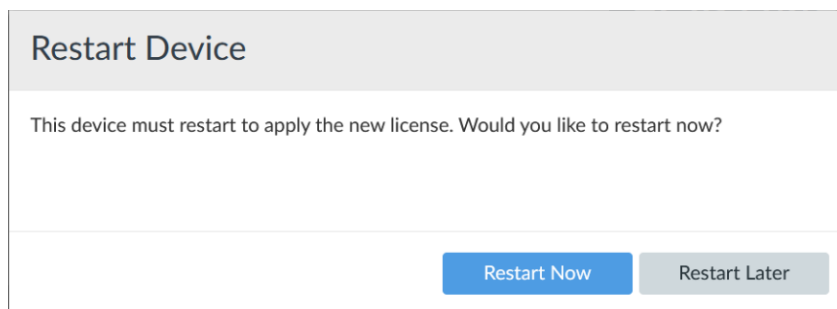




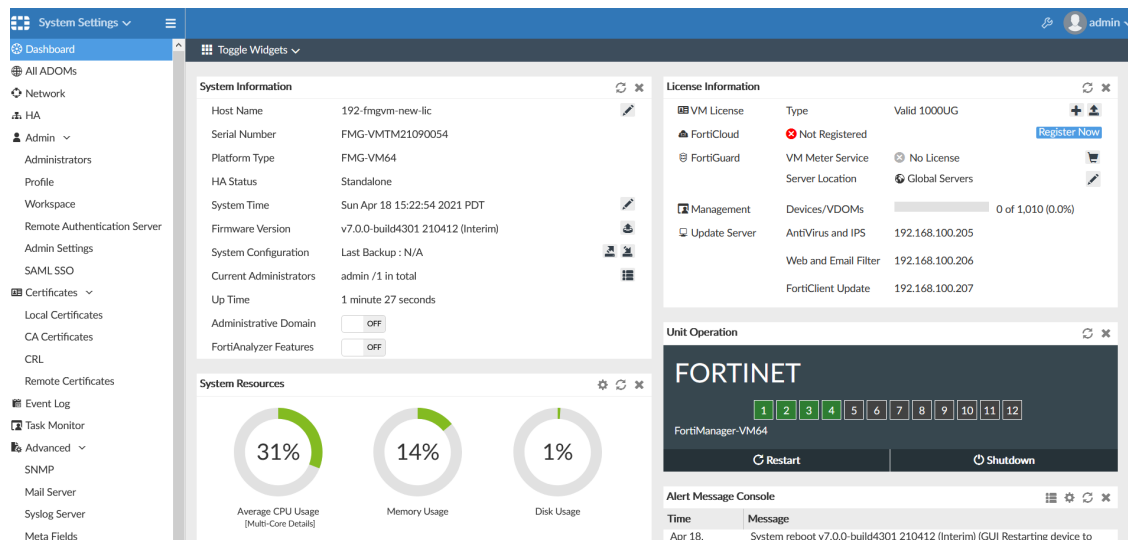
3. Complete the following options, and click OK:
    - a. In the *Account ID/Email* box, type the email for your FortiCloud account.
    - b. In the *Password* box, type the password for your FortiCloud account.
    - c. In the *Registration Code* box, enter the contract registration code for the add-on license.
- The *License Agreement* is displayed.



4. Accept the license agreement:
    - a. Read the license agreement.
    - b. Select the *I have read and accept the terms in the License Agreement* checkbox.
    - c. Click OK.
- The *Restart Device* dialog box is displayed.



5. Click *Restart Now* to apply the license.  
FortiAnalyzer restarts, and the license is applied.
6. Go to *System Settings > Dashboard > License Information* widget.  
The *VM License* option displays *Valid 1000UG*.



## FortiAnalyzer Federation

FortiAnalyzer 7.0.0 includes support for FortiAnalyzer Federation.

Configuring a FortiAnalyzer in supervisor mode provides an aggregated view of the devices, events, and incidents of each member FortiAnalyzer. Each member in the federation handles workloads and generate analytics.

This topic includes the following:

- [Device Manager on page 110](#)
- [FortiSoC on page 111](#)
  - [Event Monitor on page 111](#)
  - [Incidents on page 114](#)
  - [Supervisor Local Events on page 115](#)
- [Configure FortiAnalyzer Federation in the CLI on page 116](#)
- [Limitations on page 116](#)

This example scenario includes one FortiAnalyzer supervisor and three FortiAnalyzer members.

## Device Manager

**To view member devices in the Device Manager:**

1. On the FortiAnalyzer Federation supervisor, go to *Device Manager*.  
The *Device Manager* lists all authorized member FortiAnalyzer device information as well as each member's registered devices and ADOMs.

| Device Manager                |                  |                     |                                   |                            |                            |      |
|-------------------------------|------------------|---------------------|-----------------------------------|----------------------------|----------------------------|------|
| Quick Access ADOM: root admin |                  |                     |                                   |                            |                            |      |
| Name                          | Serial Number    | Platform            | Firmware Version                  | Max Storage                | Analytics Usage (Used/Max) |      |
| FAZVM64-Shawn-130-change      | FAZVMSTM21000390 | FortiAnalyzer-VM64  | v7.0.0-build0043 210416 (Interim) | 491.15GB                   | -                          |      |
| root                          |                  |                     |                                   | 40.0 GB                    | 24.6 GB/28.0 GB            | 88%  |
| Device Name                   | IP Address       | Platform            | Logs                              | Average Log Rate(Logs/Sec) | Device Storage             | Desc |
| Van_Office_FW1_Master         | 10.2.0.250       | FortiGate-3600E     | Real Time                         | 836                        | 87.61%                     |      |
| root                          |                  | vdom                | Real Time                         | 836                        | 87.61%                     |      |
| EMS-Lab                       | 192.168.125.1    | FortiClient-EMS     | Real Time                         | N/A                        | 0.01%                      |      |
| root                          |                  | vdom                | Real Time                         | N/A                        | 0%                         |      |
| default                       |                  | vdom                | Real Time                         | N/A                        | 0.01%                      |      |
| Shawn-CSF                     |                  |                     |                                   |                            |                            |      |
| FW-93                         | 10.2.125.223     | FortiGate-ARM64-KVM | Real Time                         | N/A                        | 0.17%                      |      |
| root                          |                  | vdom                | Real Time                         | N/A                        | 0.17%                      |      |
| FW-FCT-93                     | 192.168.125.1    | FortiGate-ARM64-KVM | Real Time                         | N/A                        | 0.34%                      |      |
| root                          |                  | vdom                | Real Time                         | N/A                        | 0.34%                      |      |
| fabric-shawn-130-1            |                  |                     |                                   | 75.0 GB                    | 533.7 MB/52.5 GB           | 1%   |
| Device Name                   | IP Address       | Platform            | Logs                              | Average Log Rate(Logs/Sec) | Device Storage             | Desc |
| FG100D3G00000099              | 10.2.125.31      | FortiGate-100D      | Real Time                         | N/A                        | 0.79%                      |      |

Each member FortiAnalyzer's tree can be expanded and collapsed. When member's device status and information is changed it will be updated on the supervisor in real-time.

| Device Manager                |                  |                    |                                   |                            |                            |      |
|-------------------------------|------------------|--------------------|-----------------------------------|----------------------------|----------------------------|------|
| Quick Access ADOM: root admin |                  |                    |                                   |                            |                            |      |
| Name                          | Serial Number    | Platform           | Firmware Version                  | Max Storage                | Analytics Usage (Used/Max) |      |
| FAZVM64-Shawn-130-change (3)  | FAZVMSTM21000390 | FortiAnalyzer-VM64 | v7.0.0-build0043 210416 (Interim) | 491.15GB                   | -                          |      |
| FAZVM64-Shawn-244 (102)       | FAZVMSTM20009250 | FortiAnalyzer-VM64 | v7.0.0-build4282 210406 (Interim) | -                          | -                          |      |
| FAZVM-S-903                   | FAZVMSTM20000056 | FortiAnalyzer-VM64 | v7.0.0-build0043 210416 (Interim) | 78.24GB                    | -                          |      |
| root                          |                  |                    |                                   | 10.0 GB                    | 6.2 GB/7.0 GB              | 89%  |
| Device Name                   | IP Address       | Platform           | Logs                              | Average Log Rate(Logs/Sec) | Device Storage             | Desc |
| FWF61E-V64                    | 10.2.60.44       | FortiWiFi-61E      | Real Time                         | N/A                        | 8.68%                      |      |
| root                          |                  | vdom               | Real Time                         | N/A                        | 8.68%                      |      |
| FGT600C                       | 10.2.60.44       | FortiGate-600C     | Real Time                         | N/A                        | 1.91%                      |      |
| root                          |                  | vdom               | Real Time                         | N/A                        | 0.4%                       |      |
| vd1                           |                  | vdom               | Real Time                         | N/A                        | 1.5%                       |      |
| lab                           |                  | vdom               | Real Time                         | N/A                        | 0.01%                      |      |
| tp                            |                  | vdom               | Real Time                         | N/A                        | 0.01%                      |      |
| FGT91E-3                      | 10.2.60.250      | FortiGate-91E      | Real Time                         | 17                         | 38.15%                     |      |
| root                          |                  | vdom               | Real Time                         | 12                         | 26.35%                     |      |
| vd1                           |                  | vdom               | Real Time                         | 4                          | 11.81%                     |      |
| nat                           |                  | vdom               | Real Time                         | N/A                        | 0.01%                      |      |

## FortiSoC

FortiSoC includes the *Event Monitor* and *Incidents* panes.

### Event Monitor

To view events from members in Event Monitor:

- On the FortiAnalyzer Federation supervisor, go to *FortiSoC > Event Monitor > All Events*. All events from members are synced to the supervisor and are organized in event groups with different time ranges. The default view lists event groups from the last day.

|                         |                               |                                     |              |            |          |       |                     |                     |
|-------------------------|-------------------------------|-------------------------------------|--------------|------------|----------|-------|---------------------|---------------------|
| FortiSoC                | Quick Access ADOM: root admin |                                     |              |            |          |       |                     |                     |
| Event Monitor           | Last 1 Day                    |                                     |              |            |          |       |                     |                     |
| All Events              | Add Filter                    |                                     |              |            |          |       |                     |                     |
| Supervisor Local Events | FAZ Name                      | Group                               | Event Status | Event Type | Severity | count | First Occurrence    | Last Update         |
| Incidents               | FAZ-VM-S-902                  | 10.5.1.2                            |              | Traffic    | Medium   | 442   | 2021-04-19 13:30:01 | 2021-04-20 13:33:32 |
|                         | FAZ-VM-S-902                  | 10.3.90.11                          |              | Traffic    | Medium   | 97    | 2021-04-19 13:30:02 | 2021-04-20 13:33:17 |
|                         | FAZVM-S-903                   | VAN-200289-US2                      | open         | DNS        | High     | 25    | 2021-04-19 12:17:53 | 2021-04-20 13:33:02 |
|                         | FAZVM-S-903                   | Intrusion from VAN-200289-US2 bl... | mitigated    | IPS        | Medium   | 14    | 2021-04-19 14:46:51 | 2021-04-20 13:33:02 |
|                         | FAZVM-S-903                   | 89.200.143.100                      | mitigated    | IPS        | High     | 6     | 2021-04-19 13:46:52 | 2021-04-20 13:33:02 |
|                         | FAZ-VM-S-902                  | 10.3.90.90                          |              | Traffic    | Medium   | 97    | 2021-04-19 13:30:01 | 2021-04-20 13:32:52 |
|                         | FAZ-VM-S-902                  | 192.168.4.2                         |              | Traffic    | Medium   | 97    | 2021-04-19 13:30:29 | 2021-04-20 13:32:44 |
|                         | FAZ-VM-S-902                  | 10.3.90.61                          |              | Traffic    | Medium   | 97    | 2021-04-19 13:30:12 | 2021-04-20 13:32:26 |
|                         | FAZVM64-Shawn-130-chan...     | 172.16.63.180                       | open         | IPS        | High     | 2     | 2021-04-19 11:16:28 | 2021-04-20 13:32:26 |

## 2. Click an event group to view associated events. You can drilldown to check event details.

FortiSoC

Event Monitor

All Events

Supervisor Local Events

Incidents

Last 1 Day

Add Filter

FAZ Name

Group

Event Status

Event Type

Severity

count

First Occurrence

Last Update

Quick Access

ADOM: root

admin

Event Group: Intrusion from VAN-200289-US2 blocked

View Log

Search in Log View

Add Filter

| <input type="checkbox"/> | FAZ Name    | ADOM Na... | Event                   | Event Status | Event Type | Count | Severity | First Occur... | Last Occur... | Additional ...  | Handler       | Tags                               | Device Na... | Acknowled... |
|--------------------------|-------------|------------|-------------------------|--------------|------------|-------|----------|----------------|---------------|-----------------|---------------|------------------------------------|--------------|--------------|
| <input type="checkbox"/> | FAZVM-S-903 | root       | Intrusion from VAN...   | mitigated    | IPS        | 2     | Medium   | 2021-04-2...   | 2021-04-2...  | Intrusion: S... | Default-Ma... | Intrusion<br>Signature<br>Attacker | FGT101E-1    | No           |
| <input type="checkbox"/> | FAZVM-S-903 | root       | Intrusion to 89.200...  | mitigated    | IPS        | 2     | Medium   | 2021-04-2...   | 2021-04-2...  | Intrusion: S... | Default-Ma... | Intrusion<br>Signature<br>Victim   | FGT101E-1    | No           |
| <input type="checkbox"/> | FAZVM-S-903 | root       | Intrusion from 10.2...  | mitigated    | IPS        | 4     | Medium   | 2021-04-1...   | 2021-04-2...  | Intrusion: S... | Default-Ma... | Intrusion<br>Signature<br>Attacker | FGT101E-1    | No           |
| <input type="checkbox"/> | FAZVM-S-903 | root       | Intrusion to 141.10...  | mitigated    | IPS        | 1     | Medium   | 2021-04-2...   | 2021-04-2...  | Intrusion: S... | Default-Ma... | Intrusion<br>Signature<br>Victim   | FGT101E-1    | No           |
| <input type="checkbox"/> | FAZVM-S-903 | root       | Intrusion to 64.37.1... | mitigated    | IPS        | 3     | Medium   | 2021-04-1...   | 2021-04-2...  | Intrusion: S... | Default-Ma... | Intrusion<br>Signature<br>Victim   | FGT101E-1    | No           |
|                          |             |            |                         |              |            |       |          |                |               |                 |               | Intrusion                          |              |              |

### 3. Select an event and click *View Log* or *Search in Log View*.

- View logs to downstream members:

The screenshot shows the FortiSoC Event Monitor interface. The top navigation bar includes 'FortiSoC', 'Event Monitor', and 'Last 1 Day'. The left sidebar has 'All Events', 'Supervisor Local Events', and 'Incidents'. The main table displays event details for a blocked intrusion.

| # | Date/Time | Device ID        | Severity | Source      | Destination IP | Action  | Service | User | Count |
|---|-----------|------------------|----------|-------------|----------------|---------|---------|------|-------|
| 1 | 12-03:32  | FG101E4Q17003... | high     | 10.2.60.117 | 141.101.115.20 | dropped | HTTP    |      |       |

Event Group: Intrusion from VAN-200289-US2 blocked

- Search in log view from downstream members:

The screenshot shows the FortiSoC Event Monitor interface with a search filter applied. The top navigation bar includes 'FortiSoC', 'Event Monitor', and 'Last 1 Day'. The left sidebar has 'All Events', 'Supervisor Local Events', and 'Incidents'. The main table displays event details for a blocked intrusion.

| # | Date/Time | Device ID        | Severity | Source      | Destination IP | Action  | Service | User | Count |
|---|-----------|------------------|----------|-------------|----------------|---------|---------|------|-------|
| 1 | 13:33:02  | FG101E4Q17003... | high     | 10.2.60.117 | 89.200.143.100 | dropped | HTTP    |      |       |
| 2 | 12-21:11  | FG101E4Q17003... | high     | 10.2.60.111 | 89.200.143.100 | dropped | HTTP    |      |       |

Event Group: Intrusion from VAN-200289-US2 blocked

Total logs for analytics: 24 days 22 hours.

#### 4. Add filters to narrow results, including filters for the FortiAnalyzer member name and group.

FortiSoC v

Event Monitor v

All Events

Supervisor Local Events

Incidents

FAZ Name = \*903\*

Filter

FAZ Name

Group

Event Status

Event Type

Severity

count

First Occurrence

Last Update

Device Name

Acknowledged

| FAZ Name    | Event Type | Severity | count | First Occurrence    | Last Update         |
|-------------|------------|----------|-------|---------------------|---------------------|
| FAZVM-S-903 | IPS        | High     | 25    | 2021-04-19 12:17:53 | 2021-04-20 13:53:21 |
| FAZVM-S-903 | Antivirus  | High     | 10    | 2021-04-19 12:15:46 | 2021-04-20 13:53:21 |
| FAZVM-S-903 | Antivirus  | High     | 9     | 2021-04-19 12:07:01 | 2021-04-20 13:53:21 |
| FAZVM-S-903 | Antivirus  | High     | 11    | 2021-04-19 12:07:01 | 2021-04-20 13:53:19 |
| FAZVM-S-903 | Event      | Medium   | 23    | 2021-04-19 14:55:41 | 2021-04-20 13:52:17 |
| FAZVM-S-903 | IPS        | Medium   | 8     | 2021-04-19 18:17:47 | 2021-04-20 13:50:29 |
| FAZVM-S-903 | IPS        | High     | 1     | 2021-04-19 22:33:41 | 2021-04-20 13:50:29 |
| FAZVM-S-903 | DNS        | High     | 18    | 2021-04-19 12:05:02 | 2021-04-20 13:50:29 |
| FAZVM-S-903 | IPS        | High     | 9     | 2021-04-19 12:01:48 | 2021-04-20 13:47:58 |
| FAZVM-S-903 | Antivirus  | High     | 12    | 2021-04-19 12:07:01 | 2021-04-20 13:37:04 |
| FAZVM-S-903 | DNS        | High     | 25    | 2021-04-19 12:01:48 | 2021-04-20 13:37:04 |
| FAZVM-S-903 | IPS        | Medium   | 14    | 2021-04-19 14:46:51 | 2021-04-20 13:33:02 |

50 /Page 1

## Incidents

### To view incidents created on members:

- On the FortiAnalyzer Federation supervisor, go to **FortiSoC > Incidents**.

All incidents raised on members can be synced to the supervisor when the member connects to the supervisor. Newly generated events are synced in real-time and updated on the supervisor.

FortiSoC v

Event Monitor v

All Events

Supervisor Local Events

Incidents

Analysis Settings

| #  | FAZ Name    | ADOM Name | Incident Number | Incident Date / Time | Incident Reporter          | Incident Category | Severity | Status   | Affected Endpoint | Description |
|----|-------------|-----------|-----------------|----------------------|----------------------------|-------------------|----------|----------|-------------------|-------------|
| 1  | FAZVM-S-903 | root      | IN00000197      | 2021-04-20 13:52:10  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.111       | Intrusi...  |
| 2  | FAZVM-S-903 | root      | IN00000196      | 2021-04-20 12:22:29  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.111       | Intrusi...  |
| 3  | FAZVM-S-903 | root      | IN00000195      | 2021-04-20 12:05:54  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | VAN-200289-US2    | Intrusi...  |
| 4  | FAZVM-S-903 | root      | IN00000194      | 2021-04-20 12:05:54  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | VAN-200289-US2    | Intrusi...  |
| 5  | FAZVM-S-903 | root      | IN00000193      | 2021-04-20 11:53:27  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.111       | Intrusi...  |
| 6  | FAZVM-S-903 | root      | IN00000192      | 2021-04-20 11:52:55  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.111       | Intrusi...  |
| 7  | FAZVM-S-903 | root      | IN00000191      | 2021-04-20 07:35:49  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | VAN-200289-US2    | Intrusi...  |
| 8  | FAZVM-S-903 | root      | IN00000190      | 2021-04-20 07:35:49  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | VAN-200289-US2    | Intrusi...  |
| 9  | FAZVM-S-903 | root      | IN00000188      | 2021-04-20 07:19:15  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.143       | Intrusi...  |
| 10 | FAZVM-S-903 | root      | IN00000189      | 2021-04-20 07:19:15  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.143       | Intrusi...  |
| 11 | FAZVM-S-903 | root      | IN00000187      | 2021-04-20 06:34:41  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | VAN-200289-US2    | Intrusi...  |
| 12 | FAZVM-S-903 | root      | IN00000186      | 2021-04-20 06:34:41  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | VAN-200289-US2    | Intrusi...  |
| 13 | FAZVM-S-903 | root      | IN00000185      | 2021-04-20 05:48:33  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.143       | Intrusi...  |
| 14 | FAZVM-S-903 | root      | IN00000184      | 2021-04-20 04:49:01  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.143       | Intrusi...  |
| 15 | FAZVM-S-903 | root      | IN00000182      | 2021-04-20 04:22:36  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.111       | Intrusi...  |
| 16 | FAZVM-S-903 | root      | IN00000183      | 2021-04-20 04:22:36  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.111       | Intrusi...  |
| 17 | FAZVM-S-903 | root      | IN00000181      | 2021-04-20 03:19:20  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.143       | Intrusi...  |
| 18 | FAZVM-S-903 | root      | IN00000180      | 2021-04-20 02:21:50  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.111       | Intrusi...  |
| 19 | FAZVM-S-903 | root      | IN00000179      | 2021-04-20 02:18:44  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.143       | Intrusi...  |
| 20 | FAZVM-S-903 | root      | IN00000178      | 2021-04-20 02:18:44  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.143       | Intrusi...  |
| 21 | FAZVM-S-903 | root      | IN00000177      | 2021-04-20 01:49:10  | Critical Intrusion Inci... | Malicious Code    | High     | Analysis | 10.2.60.143       | Intrusi...  |

- Double-click on an incident to view the incident analysis page.  
The incident analysis page displays detailed incident information.

The screenshot displays the FortiSoC incident analysis page. The left sidebar shows the navigation menu with 'Incidents' selected. The main content area is divided into several sections:

- Affected Endpoint/User:** Displays details for the incident, including 'Last Seen' (2021-04-19 19:19:42), 'Topology' (10.2.60.143), 'Addresses' (MAC: 00:0c:29:04:48:6a, IP: 10.2.60.143), and 'Operating System' (Windows XP (x86)).
- Executed Playbooks:** A table with columns 'PLAYBOOK', 'STATUS', and 'TRIGGER'. An 'Execute Playbook' button is visible.
- Incident Timeline:** A timeline showing events from 2021-04-14 06:17:19 to 2021-04-19 19:17:47 (Total 254 Events). A 'Reset Zoom' button is present.
- Audit History:** A vertical timeline showing events including 'Events Attached to Incident', 'Report Attached to Incident', and 'New Incident Created'.

- Check each attachment in the incident analysis page (Events, Reports, Affected Assets, etc). Attachments are synced from members to the supervisor.

The screenshot displays the FortiSoC incident analysis page, focusing on the 'Incident Timeline' section. The timeline shows events from 2021-04-14 06:17:19 to 2021-04-19 19:17:47 (Total 254 Events). Below the timeline, there is a table with columns: Report Name, Format, Time Range, Devices, and Status. The table shows a report named 'Bandwidth and Application...' in PDF format, covering the time range 2021/04/18 - 2021/04/19, affecting 12 Devices, with a status of 4s.

## Supervisor Local Events

### To view supervisor local events:

- On the FortiAnalyzer Federation supervisor, go to *FortiSoC > Event Monitor > Supervisor Local Events*. Local events from the supervisor are displayed.

| # | Event                           | Event Status | Event Type | Count | Severity | First Occurrence    | Last Update         | Additional Info                  | Handler         |
|---|---------------------------------|--------------|------------|-------|----------|---------------------|---------------------|----------------------------------|-----------------|
| 1 | System time modified (1)        |              | Event      | 1     | Medium   | 2021-04-19 17:34:35 | 2021-04-19 17:34:35 | system time changed: Mon A...    | Local Device Ev |
| 2 | FortiAnalyzer license limit ... |              | Event      | 1     | Medium   | 2021-04-19 12:05:36 | 2021-04-19 12:05:36 | License validation state chan... | Local Device Ev |
| 3 | Image upgrade status (1)        |              | Event      | 1     | Medium   | 2021-04-19 11:50:24 | 2021-04-19 11:50:24 | Upgrade image from v7.0.0-b...   | Local Device Ev |

## Configure FortiAnalyzer Federation in the CLI

### To configure a FortiAnalyzer Federation supervisor:

1. In the supervisor CLI, enable soc-fabric communication:
 

```
config system interface
edit port1
set allowaccess soc-fabric
```
2. Enter the following commands to configure the supervisor:
 

```
config system soc-fabric
set status enable
set role supervisor
set name <create the FortiAnalyzer Federation name>
set psk <create the FortiAnalyzer Federation password>
set port 6443 (set the communication port if not using the default value)
set secure-connection enable
```

Multiple FortiAnalyzer devices can be configured as members. Each FortiAnalyzer in Analyzer mode must be individually configured as a member to participate in the FortiAnalyzer federation.

### To configure a FortiAnalyzer Federation member:

1. In the member CLI, enable soc-fabric communication:
 

```
config system interface
edit port1
set allowaccess soc-fabric
```
2. Enter the following commands to configure the member:
 

```
config system soc-fabric
set status enable
set role member
set name <enter the FortiAnalyzer Federation name>
set psk <enter the FortiAnalyzer Federation auth password>
set supervisor ip <enter the IP/FNDN of the supervisor>
set port 6443 <set the communication port if not using the default one>
set secure-connection enable
```

## Limitations

- FortiAnalyzer Federation supports the creation of incidents, event handlers, and events on members with centralizing viewing from the supervisor.
- FortiAnalyzer Federation supports log analysis, including *LogView* and *Reports*, on FortiAnalyzer Federation members.



- Incidents on the FortiAnalyzer Federation supervisor are available in read-only mode.
- FortiAnalyzers configured in high availability (HA) mode can join the FortiAnalyzer Federation as members. HA is not supported for FortiAnalyzer Federation supervisors.
- All FortiAnalyzer Federation members must be configured with the same timezone settings as the supervisor.

## CSF support for multiple VDOMs

Multiple VDOMs can now form a Security Fabric Cluster.

### To view multiple VDOMs in a CSF on FortiAnalyzer:

- In the FortiAnalyzer *Device Manager*, add a FortiGate running 7.0.0 which has enabled Multi VDOM mode in an ADOM.

After a few moments, the *Device Manager* will display the Central Security Fabric with configured VDOMs.

| Device Name       | IP Address  | Platform       | Logs      | Average Log Rate(Logs/Sec) | Device Storage | Description |
|-------------------|-------------|----------------|-----------|----------------------------|----------------|-------------|
| ✖ Fabric700       |             |                |           |                            |                |             |
| FortiGate-VM-212* | 10.4.90.212 | FortiGate-VM64 | Real Time | N/A                        | (0%)           |             |
| root              |             | vdom           | Real Time | N/A                        | (0%)           |             |
| vd1               |             | vdom           | Real Time | N/A                        | (0%)           |             |
| vd2               |             | vdom           | Real Time | N/A                        | (0%)           |             |
| FortiGate-VM-213  | 10.4.90.213 | FortiGate-VM64 | Real Time | N/A                        | (0%)           |             |
| FG-traffic        |             | vdom           | Real Time | N/A                        | (0%)           |             |
| root              |             | vdom           | Real Time | N/A                        | (0%)           |             |

## Event log easier to read - 7.0.1

The FortiAnalyzer event log includes the following new columns to make messages easier to read:

- Operation*
- Performed On*
- Changes*

Go to *System Settings > Event log* to view the new columns:

| # | Date Time           | Level       | User                  | Sub Type | Description                                             | Operation       | Performed On    | Changes                                                                                                                          |
|---|---------------------|-------------|-----------------------|----------|---------------------------------------------------------|-----------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| 1 | 2021-04-29 10:22:29 | information | update_manager        | fgd      | Package update response from FortiGuard server received | Update Response | 12.34.97.16     | Receive an update package from fds(000000.00000-2104291723): 01000000ALC00000(ALCI Object), version:00000.00000-2104291723       |
| 2 | 2021-04-29 10:13:43 | information | admin-GUI(10.2.0.250) | system   | User login/logout successful                            | login           | GUI(10.2.0.250) | 'admin' login accepted from GUI(10.2.0.250)                                                                                      |
| 3 | 2021-04-29 10:13:42 | information | fgdlinkd              | fgd      | Package update response from FortiGuard server received | Update Response | FDS Server      | Receive an update package from FDS: (CURL000000FortiGuard CURL),version:00001.00060-2001131740                                   |
| 4 | 2021-04-29 10:12:17 | information | update_manager        | fgd      | Package update response from FortiGuard server received | Update Response | 12.34.97.16     | Receive an update package from fds(000000.00000-2104291713): 01000000ALC00000(ALCI Object), version:00000.00000-2104291713       |
| 5 | 2021-04-29 10:05:23 | notice      | System                | dvm      | Device Manager dvm log at notice level                  | Modify device   | FGVM4VTM20...   | Edited device settings (SN FGVM4VTM20003032)                                                                                     |
| 6 | 2021-04-29 10:05:12 | notice      | System                | dvm      | Device Manager dvm log at notice level                  | Modify device   | FGVM4VTM20...   | Edited device settings (SN FGVM4VTM20003032)                                                                                     |
| 7 | 2021-04-29 10:01:55 | information | update_manager        | fgd      | Package update response from FortiGuard server received | Update Response | 12.34.97.16     | Receive an update package from fds(000000.00000-2104290050): 06004000AP0800100(Application Meta), version:00018.00070-2104290050 |
| 8 | 2021-04-29 10:01:55 | information | update_manager        | fgd      | Package update response from FortiGuard server received | Update Response | 12.34.97.16     | Receive an update package from fds(00018.00070-2104290054): 06000000NID502500(IPS Extended Meta), version:00018.00070-2104290054 |
| 9 | 2021-04-29 10:01:55 | information | update_manager        | fgd      | Package update response from FortiGuard server received | Update Response | 12.34.97.16     | Receive an update package from fds(00018.00070-2104290054): 06000000NID502400(IPS Regular Meta), version:00018.00070-2104290054  |



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.